KEY CHALLENGES OF HEALTHCARE IOT GOVERNANCE

BERK COŞARDEMİR

BOĞAZİÇİ UNIVERSITY

2025

KEY CHALLENGES OF HEALTHCARE IOT GOVERNANCE

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Management Information Systems

by

Berk Coşardemir

Boğaziçi University

2025

Key Challenges of Healthcare IoT Governance

The thesis of Berk Coşardemir

has been approved by:

Prof. Bilgin Metin
(Thesis Advisor) _____

Assoc. Prof. Nazım Taşkın _____

Assist. Prof. Arafat Salih Aydıner
(External Member) _____

June 2025

DECLARATION OF ORIGINALITY

I, Berk Coşardemir, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature……...

Date…….....

ABSTRACT

Key Challenges of Healthcare IoT Governance

Smart healthcare uses IoT devices and cloud analytics to improve diagnosis and workflow, yet these tools heighten cyber risks, widen interoperability gaps, complicating compliance. Conventional IT governance assumes stable systems, overlooking device control, latency, and user adoption, while most IoT frameworks focus solely on security, ignoring clinical realities. This study uses a sequential explanatory mixed-methods strategy: a systematic literature review of 76 papers and interviews with seven experts from Turkiye. Analysis of 13 key IoT challenges, along with current healthcare reference architectures and governance frameworks, reveals three critical gaps: real-time performance assurance, fragmented device-lifecycle control, and limited user engagement. In response, this study introduces Govern-IoT-Health, a governance construct melding the Human-Organization-Technology (HOT-fit) cube with a central Governance-Risk-Compliance (GRC) spine and an explicit Plan-Do-Check/Act (PDC) loop. Its three orthogonal faces align people, structure, and infrastructure, while the GRC core embeds board-level policy, real-time telemetry, and automated compliance checks. Twenty-eight defined mechanisms populate the PLAN, DO, and CHECK & ACT stages. Building on established standards including ISO 27001, ISO/IEC 30141, NIST IR 8259A, HL7 FHIR, ETSI EN 303 645, HIPAA, and GDPR, the framework adds SBOM controls and continuous monitoring atop a curated catalogue of reference architectures (classical three-layer, edge-oriented, multi-layer/service-oriented, security-focused, and standards-aligned). Govern-IoT-Health offers a practical, standards-aligned route to secure IoT deployment.

ÖZET

Sağlık IoT Yönetişimindeki Temel Zorluklar

Akıllı sağlık hizmetleri, teşhis ve iş akışını iyileştirmek için IoT cihazları ve bulut analitiğinden yararlanmaktadır; ancak bu araçlar siber riskleri, birlikte çalışabilirlik açıklarını ve uyumluluğu zorlaştırmaktadır. Geleneksel BT yönetişimi bu gibi dinamikleri göz ardı ederek durağan sistemleri varsayarken, mevcut IoT çerçevelerinin çoğu yalnızca güvenliğe odaklanıp klinik gerçeklikleri dikkate almamaktadır. Bu çalışma, sistematik literatür taraması ve uzman görüşmelerini içeren karma yöntem stratejisini benimsemektedir. 13 temel IoT zorluğu ile mevcut çerçevelerin analizi sonucunda üç temel boşluk belirlenmiştir: gerçek zamanlı performans güvencesi, parçalı cihaz yaşam döngüsü kontrolü ve sınırlı kullanıcı katılımı. Bu kapsamda çalışma, İnsan-Organizasyon-Teknoloji (HOT-fit) küpünü merkezi bir Yönetişim-Risk-Uyumluluk (GRC) omurgası ve Planla-Uygula-Kontrol Et/Önlem Al (PDC) döngüsüyle birleştiren Govern-IoT-Health'i önermektedir. Küpün yüzeyleri insan, yapı ve altyapıyı hizalarken; GRC çekirdeği politikaları, gerçek zamanlı telemetri ve otomatik uyumluluk kontrollerini entegre eder. PDC aşamalarına dağıtılmış 28 mekanizma içermektedir. ISO 27001, ISO/IEC 30141, NIST IR 8259A, HL7 FHIR, ETSI EN 303 645, HIPAA ve GDPR gibi yerleşik standartlara dayanan çerçeve; yazılım bileşen listesi (SBOM) kontrolleri ve sürekli izleme mekanizmalarını, çeşitli referans mimarilerden oluşan bir katalog üzerine inşa eder. Govern-IoT-Health, güvenli IoT uygulamaları için pratik ve standartlara uygun bir yol sunmaktadır.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor, Professor Bilgin Metin, for his unwavering guidance, readily available support, and boundless patience. His insight and constructive feedback were instrumental.

I am equally indebted to Associate Professor Nazım Taşkın and Assistant Professor Arafat Salih Aydıner for their encouragement, insightful comments, and generous investment of time. Their scholarly rigor and thoughtful perspectives sharpened the arguments in this dissertation.

I would like to express my sincere gratitude to Borda Technology for the valuable professional experience that contributed to this work, and to my former colleagues, whose insights and participation made it possible.

Special appreciation goes to my friend Can Erhan for his constant availability and steadfast support; without his encouragement, I might never have embarked on this journey. I also thank Elçin Polen Günay, whose contribution and creative visual expertise greatly enhanced this work. Thanks as well to Ayhan Kayan for promptly solving a challenging logistic problem without hesitation on very short notice.

My deepest thanks go to my family for believing in me and standing by me. To my mother, whose constant love sustained me, and to the cherished memory of my father. I am also grateful to my brother and sister for their unwavering encouragement.

Finally, I extend my heartfelt appreciation to my beloved life partner, Elif Bike Osun, whose endless patience, limitless support, and courageous pushes kept me moving forward. To our soon-to-be-born son, whose very existence has already filled me with purpose and motivation, this work is lovingly dedicated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Smart healthcare concept refers to a modern healthcare model that has evolved through the digital transformation of the healthcare industry. Smart healthcare leverages advanced technology and data-driven solutions to improve patient care, optimize hospital operations, and enhance the overall healthcare experience. This concept is powered by key technologies, including Internet of Things (IoT) for real-time connectivity, data analytics for informed decision-making, personalized services for individual patient needs, and Artificial Intelligence to enhance diagnostics and predictive care (Uslu et al., 2020). Among these technologies, smart hospitals heavily rely on IoT technologies to create interconnected environments to collect accurate and reliable data. These collected data are then useful to perform data analysis, ultimately making critical decisions for effective healthcare applications. From a broader perspective, IoT applications can be categorized in various healthcare settings, which are indoor environments, outdoor environments, and remote patient monitoring (Li et al., 2024).

Despite these advantages, integrating IoT into healthcare introduces several challenges. Security and privacy are major concerns, as sensitive patient data collected by IoT devices can be vulnerable to unauthorized access and cyber threats (Darshan & Anandakumar, 2015). Additionally, interoperability and a lack of standardized protocols complicate seamless integration among diverse devices and systems (Hussain, 2017). Managing the large volume of data continuously generated from IoT devices requires scalable storage and efficient processing to maintain real-time performance (Mishra & Singh, 2023). Further challenges include energy

efficiency, particularly with battery-powered wearable devices, and ensuring compliance with regulatory standards to safeguard patient safety and data privacy (Selvaraj & Sundaravaradhan, 2020).

To address the challenges of IoT in healthcare, it is necessary to use specific IoT governance frameworks rather than traditional IT governance methods. Although traditional frameworks like COBIT, ITIL, and ISO/IEC 27001 are useful they do not fully cover the unique needs of IoT technology, such as managing devices, handling large amounts of data, and specific privacy and security concerns (Almeida et al., 2015; Copie et al., 2013; Sedrati et al., 2023). Although emerging IoT-specific frameworks introduce layered architectures and processes suited to heterogeneous sensors and real-time data streams, they are typically sector-agnostic and rarely incorporate the stringent safety, clinical effectiveness, and multi-jurisdictional privacy duties demanded in healthcare, nor do they align comprehensively with HIPAA, GDPR, or medical-device regulations (Baker et al., 2017). Consequently, neither class of framework can by itself ensure that connected medical devices remain secure, interoperable, and clinically trustworthy throughout their lifecycle; a dedicated healthcare IoT governance model is therefore required one that delineates responsibilities, rules, transparency, and accountability across devices, communications, platforms, and applications while integrating patient-centric, regulatory, and ethical imperatives with the technical depth of IoT governance (Al-rawashdeh et al., 2022; Weber, 2016).

Recognizing these gaps, first, a systematic literature review synthesizes published evidence on IoT reference architectures, challenges, and governance frameworks in healthcare. Second, to capture practitioner perspectives that literature alone may overlook, we conducted seven semi-structured interviews with hospital IT

directors, IT project managers, and healthcare IoT technology providers' COO, directors, project managers, and biomedical engineers. The interview protocol explored real-world governance practices, perceived IoT challenges, and expectations for effective frameworks, thus enriching the SLR findings with context-specific insights and gathering evidence from multiple sources.

The objectives of this research are fourfold. First, examine why healthcare settings require dedicated IoT reference architectures and catalogue the architectures' characteristics that already exist. Second, identify the principal challenges associated with implementing IoT in healthcare systems. Third, evaluate current governance frameworks find out how well they address those challenges within healthcare IoT environments. Finally, it proposes an improved governance framework designed specifically to meet the identified challenges of IoT in healthcare. This study will answer the following research questions to achieve its objectives:

RQ1. Why are IoT reference architectures needed in healthcare, and what are the existing architecture types?

RQ2. Which governance frameworks are used for IoT governance, and what do they address in IoT healthcare?

RQ3. How can a new IoT governance framework be developed to address the challenges of IoT in healthcare?

This thesis provides a comprehensive exploration of IoT governance frameworks specifically tailored for healthcare applications. The study begins with an introduction highlighting the necessity of specialized IoT governance frameworks for healthcare, given the inadequacy of traditional IT governance methods. The research combines a systematic literature review with seven semi-structured expert interviews. Building on these methods, it also includes a systematic analysis of IoT

reference architectures and governance frameworks, comparing them with expert opinions to identify points of agreement and disagreement. The findings and analysis section uses this input to evaluate current governance practices and highlight critical gaps. Subsequently, a proposed IoT Healthcare Governance Framework is introduced to effectively address the identified challenges. A sample case study demonstrates the practical application of the Govern-IoT-Health framework. Finally, the discussion section reflects on the framework's potential implications, limitations, and areas for future research.

CHAPTER 2

BACKGROUND

This chapter reviews the current state of the healthcare IoT governance literature. It begins by outlining the emergence of smart healthcare as a model that integrates digital technologies, data systems, and connected medical devices to improve clinical outcomes and operational efficiency. The role of IoT technologies within this model is then explained, with particular attention to the technical components that support real-time data exchange, remote monitoring, and decision support. The challenges that arise from these developments are identified next, including ongoing concerns around data security, patient privacy, interoperability, and organizational complexity. To address these issues, established IT governance frameworks and ISO/IEC standards are then examined, offering insight into existing mechanisms for aligning technology with business objectives and regulatory demands. These are further explored in the context of IoT governance, where adaptations have been proposed but remain inconsistently applied. The discussion then turns to healthcare-specific standards and regulations, highlighting sectoral requirements such as GDPR, HIPAA, and IEC 82304-1 that influence governance design. Finally, the literature is reviewed to assess calls for a dedicated governance framework tailored to the unique needs of healthcare IoT, where existing models often fall short in addressing the interplay between technical constraints, regulatory obligations, and stakeholder coordination.

2.1 Smart healthcare applications

Smart healthcare concept refers to a modern healthcare model that has evolved through the digital transformation of the healthcare industry. Smart healthcare leverages advanced technology and data-driven solutions to improve patient care, optimize hospital operations, and enhance the overall healthcare experience. This concept is powered by key technologies, including Internet of Things (IoT) for real-time connectivity, data analytics for informed decision-making, personalized services for individual patient needs, and Artificial Intelligence to enhance diagnostics and predictive care (Uslu et al., 2020). Among these technologies, smart hospitals heavily rely on IoT technologies to create interconnected environments to collect accurate and reliable data. These collected data are then useful to perform data analysis, ultimately making critical decisions for effective healthcare applications. From a broader perspective, IoT applications can be categorized in various healthcare settings, which are indoor environments, outdoor environments, and remote patient monitoring (Li et al., 2024). Smart application categories and their example applications are shown in Figure 1.

Hospitals and medical facilities can be considered as indoor healthcare environments. This setting focuses on creating an interconnected ecosystem to enhance patient care, optimize resources, and improve operational efficiency (Li et al., 2024). In this category, the key applications include smart monitoring systems where IoT devices track patient vitals and send alerts to healthcare providers. Medical devices such as heart rate monitors, glucose meters, and ECG machines can send real-time data to central systems via Wi-Fi (Yang et al., 2016). Resource and asset tracking is another application group in which the IoT sensors can help locate medical equipment, ensure inventory management, and reduce unnecessary costs

(Ramson et al., 2020). It can be exemplified as tagging and tracking medical equipment such as infusion pumps, defibrillators, and wheelchairs to ensure proper utilization and location tracking. Environmental control applications indicate that systems implemented in smart hospitals maintain optimal lighting, temperature, and air quality to ensure patient comfort and safety. In the indoor setting, the usage of IoT technologies may be different than those used in the other settings. For example, short-range technologies such as Bluetooth or Wi-Fi are suitable for these kinds of applications.

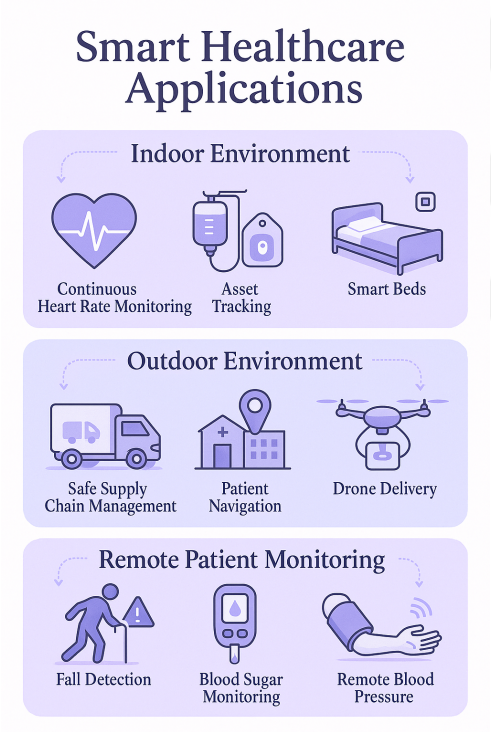

Figure 1. Smart healthcare applications

In addition to applications in indoor environments, outdoor healthcare environments play a significant role in the overall healthcare experience. Outdoor settings include areas where IoT facilitates care delivery and logistics beyond hospital walls. Recreational areas, public spaces around healthcare facilities, parking,

and transportation locations can be exemplified for this case. Common applications include safe supply chain management of medical supplies such as vaccines and blood sample monitoring, their temperature, and location (Nanda et al., 2023). IoT-enabled information desks can help patients and visitors navigate the facility and manage their experience without spending too much time (Ramson et al., 2020). Outdoor spaces generally require long-range and low-power IoT technologies such as NB-IoT or LTE-M for seamless operation and maintenance.

Remote patient monitoring is another application area of IoT in healthcare. It refers to collecting patient health data outside of the traditional clinical settings. This approach enables healthcare providers to monitor, assess, and manage patient conditions remotely to ensure continuous care. For example, chronic disease management enables continuous monitoring of conditions like diabetes, hypertension, and heart disease. Wearable IoT devices play a pivotal role. They allow continuous monitoring of vital signs such as heart rate, blood pressure, or blood sugar of the patients that are being tracked (Al Shorman et al., 2020). Fall detection is another application where the system can automatically alert healthcare providers when a fall is detected.

2.2 IoT technologies

Internet of Things (IoT) refers to a network of interconnected devices that communicate and exchange data over the internet. This technology provides seamless integration between the physical and digital worlds. IoT devices can interact with each other and the environment. In the late 1990s, IoT evolved from a theoretical concept to a practical reality. Over the years, IoT has expanded into sophisticated applications leveraging advancements in wireless communication,

cloud computing, and artificial intelligence (Zanella et al., 2014). IoT plays a central role in Industry 4.0 by enabling the connection and communication of machines, sensors, and devices in manufacturing environments. By 2023, the number of IoT devices was projected to reach 45 billion, which highlights its rapid adoption across industries (Vijayakumaran et al., 2020).

IoT technologies provide a diverse range of protocols that enable devices to communicate, collect, and exchange data across various areas, especially for healthcare. These protocols are crucial for ensuring interoperability, data exchange, security, and efficient communication across different IoT devices and networks. The choice of a suitable protocol depends on the specific requirements of the IoT application, such as range, power consumption, and data transfer rate. There are two basic IoT protocols, which are communication and application protocols.

The communication protocols of IoT technology can be broadly categorized based on their range and power consumption into two major groups: Low-Power Wide-Area Networks (LPWAN) and Short-Range Communication Protocols (Al-Sarawi et al., 2017). This classification reflects the diverse requirements of IoT applications, ranging from localized to long-distance data exchanges and low-power communication. Table 1 and Table 2 present a detailed comparison of LPWAN and Short-range Communication Protocols, respectively. These tables summarize key features such as data rates, power consumption, communication range, and several application areas. Each IoT protocol has its own set of advantages and disadvantages, making them suitable for specific application areas.

The Internet of Things (IoT) in healthcare relies on various communication protocols tailored to the resource limitations and interoperability demands of medical environments. The Constrained Application Protocol (CoAP), derived from the

REST architecture, is optimized for devices with limited resources by modifying HTTP features to support lightweight, RESTful communication (Lin et al., 2017). MQTT (Message Queue Telemetry Transport) employs a publish/subscribe model and is highly efficient in environments with constrained bandwidth and high latency, making it suitable for transmitting sensor data (Al-Fuqaha et al., 2015). XMPP (Extensible Messaging and Presence Protocol) enables decentralized, secure, and extensible messaging, commonly used for instant messaging and communication services. AMQP (Advanced Message Queuing Protocol) offers message reliability through standardized messaging over TCP, supporting both publish/subscribe and point-to-point models (Al-Fuqaha et al., 2015; Lin et al., 2017). Finally, HL7 (Health Level Seven) is a healthcare-specific protocol that enables interoperability by standardizing electronic health data formats and structures across diverse systems, improving communication among both standard and nonstandard devices (Koutras et al., 2020).

Table 1. IoT Communication Technologies - LPWAN

Attribute	NB-IoT	LTE-M	LoRaWAN	SigFox
Standard	LTE	LTE	LoRa	SigFox
Frequency Bands	450 MHz - 2 GHz	450 MHz - 3.6 GHz	863 - 873 MHz	868 - 928 MHz
Power	Low Power	Low Power	Low Power	Low Power
Latency	1.6-10s	10-15ms	Seconds	Seconds
Data Rate	16.9 Kbps- 159 Kbps	1 Mbps-7 Mbps	50 Kbps	100 bps
Range	1-10 Km	1-10 Km	1-15 Km	3-50 Km
Security	3GPP (128-256 bit)	3GPP (128-256 bit)	AES-128	AES-128
Application Areas	Utilities and Energy, Smart Cities, Smart Homes, Industrial IoT, Agriculture	Asset Tracking and Supply Chain, Utilities and Energy, Smart Cities, Smart Homes, Industrial IoT, Agriculture	Industrial IoT, Smart Cities, Utilities and Energy, Agriculture	Asset Tracking and Supply Chain, Smart Cities, Utilities and Energy, Agriculture

Table 2. IoT Communication Protocols - Short Range

Attribute	ZigBee	Bluetooth	RFID	NFC	Z-Wave	UWB	Wi-Fi	6LoWPAN
Standard	IEEE 802.15.4	IEEE 802.15.1	RFID	ECMA 340	Z-Wave	IEEE 802.15.4a	IEEE 802.11	IEEE 802.15.4
Frequency Bands	868 - 928 MHz / 2.4 GHz	2.4 GHz	125-134.2 kHz (LF), 13.56 MHz (HF), 860-960 MHz (UHF)	13.56 MHz	800 - 900 MHz	3.1 - 10.6 GHz	2.4 Ghz 5 GHz 6 GHz	2.4 Ghz
Power	Low Power	Low Power (BLE)	Ultra-Low Power	Ultra-Low Power	Low Power	Low Power	High Power	Low Power
Latency	100 - 200 ms	100 - 200 ms	10ms-seconds	100 - 250 ms	100 - 500 ms	1-2 ms	1 - 100 ms	10-100 ms
Data Rate	20-250 Kbps	1 Mbps	1-2 Kbps (LF), 26-848 Kbps (HF), 640 Kbps (UHF)	424 Kbps	40 Kbps	1 Gbps	10 Gbps	2 - 250 Kbps
Range	5-500 m	10-100 m	10 cm (LF), 1 m (HF), 10 m (UHF)	4 cm - 10 cm	30 - 100 m	10 - 100 m	70 - 250 m	10 - 100 m
Security	AES-128	AES-128	RC4	RSA AES	AES-128	AES RSA	WPA2 WPA3	AES-128
Application Areas	Industrial IoT, Smart Cities, Utilities and Energy, Smart Home	Healthcare, Industrial IoT, Smart Home	Asset Tracking and Supply Chain, Personal Identification	Personal Identification, Contactless Payments, Healthcare	Smart Home	Location-Based Services, Healthcare, Smart Home, Industrial IoT	Smart Home, Smart Cities, Healthcare, Industrial IoT, Agriculture	Smart Home, Utilities and Energy, Healthcare, Industrial IoT

2.3 IoT challenges

The expanding use of IoT in healthcare presents both advancements and challenges. There is an increasing number of protocols and technologies being developed and widely adopted in the IoT domain, introducing complexities (R. Khan et al., 2012). Some important issues are security and privacy, data management, device management, interoperability and standardization, and regulatory and legal considerations (Kumar et al., 2019; Syed et al., 2021; Y. Yang et al., 2017). Among these, one of the biggest challenges is the diversity of devices and data, which affects the ability to integrate and manage various IoT devices effectively in healthcare systems (Bedhief et al., 2016). Addressing these challenges needs strategies that balance innovation with robust governance frameworks.

2.4 IT governance frameworks, best practices, and ISO/IEC standards

Modern organizations depend on structured governance frameworks and internationally ratified standards to steer information technology toward strategic goals while maintaining security, privacy, and regulatory compliance. Practitioner frameworks such as the Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT) supply process-oriented guidance for service management and risk oversight, whereas the ISO/IEC families extend this guidance with normative requirements and reference architectures that formalize controls across security management systems (ISO/IEC 27000), Internet-of-Things security and privacy (ISO/IEC 27400-series), and system design principles (ISO/IEC 30141) (ISO/IEC, 2022b; Khther & Othman, 2013; Peña et al., 2013). Together, these instruments create a coherent governance toolkit that translates high-level principles into auditable practices, helping

organizations optimize resources, assure stakeholders, and adapt to rapid technological change. The following subsections examine each framework and standard in turn, clarifying their scope, structure, and contribution to a comprehensive IT governance strategy.

2.4.1 The Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a widely adopted framework for IT service management (AXELOS, 2019). ITIL was first created by the UK's Office of Government Commerce (OGC) to improve IT operations in the public sector. ITIL is now maintained by the Information Technology Service Management Forum (ITSMF) and focuses on transforming IT departments into service-oriented organizations. The framework is organized into five core areas, with each area detailed in separate guidance books: Service Strategy (SS), Service Design (SD), Service Transition (ST), Service Operation (SO), and Service Continual Improvement (SCI). This lifecycle approach combines development and operations, supporting continuous improvement in IT service delivery. Although ITIL offers detailed processes for managing IT services, it does not focus on measuring IT quality and is often utilized as a framework for service delivery (Peña et al., 2013).

2.4.2 Control Objectives for Information and Related Technologies (COBIT)

COBIT (ISACA, 2019) is a widely used IT governance framework that provides methodologies for managing IT risks, aligning IT operations with business objectives, and ensuring regulatory compliance. It offers a comprehensive set of best practices that organizations can use to create control policies and improve IT decision-making. COBIT splits IT governance into four domains: planning,

implementation, service delivery, and evaluation, with organized processes supporting each area. Integrating industry standards and providing performance measurement tools, COBIT helps organizations optimize their IT resources while maintaining security and efficiency (Khther & Othman, 2013).

2.4.3 ISO/IEC 27000 family

ISO/IEC 27000 is a collection of standards designed to establish best practices for information security management. This framework provides guidelines and recommendations for organizations. It aims to enhance information security across various domains. The series consists of 46 interrelated standards. ISO 27001 and ISO 27002 are the most widely known for their role in defining information security management systems (ISMS). Similar to frameworks like COBIT and ITIL, ISO 27000 outlines governance principles, including roles, responsibilities, and policies (Sedrati et al., 2023).

2.4.4 ISO/IEC 27400 2022 Cybersecurity-IoT security and privacy guidelines

ISO/IEC 27400:2022 is an international security standard that provides guidelines and best practices for security and privacy in IoT. It outlines security risks, threat mitigation strategies, and privacy considerations for IoT ecosystems. It contributes to safer deployment of IoT across various industries, including healthcare, smart cities, and industrial automation. This standard aims to address device vulnerabilities, data protection challenges, and interoperability issues (ISO/IEC, 2022b).

2.4.5 ISO/IEC 27402 2023 Cybersecurity-IoT security and privacy- Device baseline requirements.

ISO/IEC 27402:2023 defines fundamental information and communication technology (ICT) requirements for IoT devices. It focuses on security and privacy measures. Developed by ISO and IEC. It aims to mitigate the security and privacy risks related to the growing adoption of IoT devices. The standard outlines essential baseline requirements to improve device security and privacy, promoting a unified global approach to IoT cybersecurity (ISO/IEC, 2023).

2.4.6 ISO/IEC 27403 2024 Cybersecurity-IoT Security and Privacy- Guidelines for IoT-Domotics

ISO/IEC 27403:2024 provides detailed guidelines for assessing security and privacy risks in IoT systems used in domestic environments, also known as domotics. It outlines specific controls to reduce these risks by tackling the challenges of integrating IoT devices in homes. It aims to improve the security and privacy of IoT-domotics systems by providing targeted recommendations (ISO/IEC, 2024b).

2.4.7 ISO/IEC 27404 Cybersecurity IoT Security and Privacy-Cybersecurity Labelling Framework for Consumer IoT

It is an upcoming international standard under development by ISO/IEC. This standard aims to develop a universal framework for cybersecurity labeling of consumer IoT products by providing guidance on assessing risks and threats, defining stakeholder roles and responsibilities (ISO/IEC, 2024c).

2.4.8 ISO/IEC 30141 Internet of Things (IoT) - Reference architecture

ISO/IEC 30141:2024 provides a reference architecture for IoT systems. It offers standardized terminology, principles, and guidelines for architectural descriptions. It ensures a unified approach to defining IoT capabilities, system interactions, and best practices. The standard is designed to support architects in developing IoT architectures and reference models by providing a structured approach to IoT system design. Additionally, its normative elements can be incorporated into practical IoT implementations with conceptual models with real-world applications (ISO/IEC, 2024a).

2.5 IT governance and IoT governance

Governance refers to the processes, structures, and systems used to guide decision-making and to effectively manage operations in a sector or organization. It involves creating policies, setting goals, and having accountability to achieve desired outcomes. IT governance refers to the framework an organization uses to oversee and control its IT systems and resources. It focuses on the decision-making process about IT, defining who makes these decisions and the methods used to make them. IT governance is responsible for setting the organization's IT goals, determining the strategies to achieve them, and monitoring progress. Corporate executives, such as the Chief Information Officer (CIO), play a key role in IT governance, but the responsibility goes beyond their role. To create alignment between business goals and IT objectives, IT governance requires collaboration with corporate executives and business managers, contrary to the misconception that the CIO alone is responsible for these decisions (Peterson, 2004).

IoT governance extends beyond traditional IT governance, involving distinct management and overseeing processes needed for the Internet of Things (IoT) ecosystem. IoT is not just a sub-category of IT, but it is an evolution that brings new challenges and opportunities, creating the need for specific governance strategies. IT governance focuses on managing IT systems, while IoT governance deals with the specific aspects of IoT, like data management and the integration of a large network of interconnected devices (see Figure 2). Core IoT governance concerns include device lifecycle management, data ownership, cybersecurity, and interoperability. Adopting innovative management approaches is essential for effective IoT governance, especially given that IoT's influence on business performance can be transformative or disruptive (Sedrati et al., 2023). Consequently, IoT reference architectures play a critical role by providing standardized, modular blueprints that guide the design, implementation, and governance of IoT systems. There are different definitions of IoT governance in the literature, illustrated in Table 3.

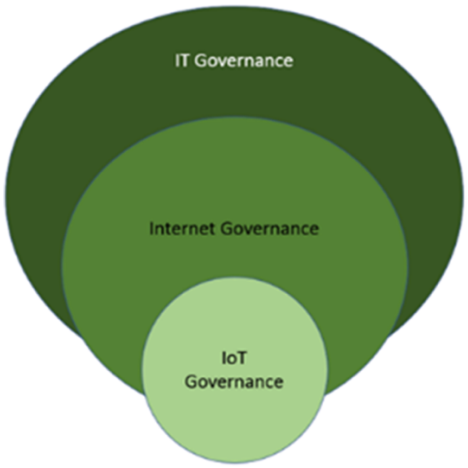

Figure 2. Relationship between IT, the internet, and IoT governance
Source: (Sedrati et al., 2023)

Table 3. IoT Governance Definitions

IoT Governance Definition (Synthesized)	Reference
IoT governance refers to the design of institutions and structures that allocate resources and control activities in society, specifically in relation to IoT technologies.	(Weber, 2013)
The process of establishing rules, norms, and regulations to ensure safety, security, and privacy in the IoT ecosystem, involving governments, civil society, the private sector, and academia to minimize risks introduced by IoT.	(Almeida et al., 2017)
IoT Governance ensures the efficient management of connected devices by enabling the addition, updating, and removal of things while handling large-scale data collection and monitoring. It oversees data aggregation using algorithms and processing techniques while prioritizing security and privacy.	(Copie et al., 2013)
IoT governance is the process of managing and overseeing the Internet of Things (IoT) by addressing its unique challenges, such as data handling and the coordination of interconnected devices. It involves creating specific strategies and policies to ensure the effective, secure, and efficient operation of IoT systems, considering their impact on business performance and innovation.	(Sedrati et al., 2023).

2.5.1 IoT Governance Frameworks

The explosion of AI-enabled connected devices has made governance a foundational requirement for the Internet of Things, on par with the importance of connectivity itself. Unlike traditional IT estates, IoT ecosystems must coordinate autonomous devices, multiple stakeholder interests, continuous data flows, and stringent regulatory obligations while maintaining accountability, transparency, and security. Several specialized frameworks, among them IoT-Gov, the 4I data governance cycle, an IoT Smart-City reference architecture, and a multi-agent governance design, have emerged to address these unique demands. The comparative analysis that follows distils their objectives, governance principles, and structural features into insights that can inform a unified model for high-risk domains such as healthcare, where a single comprehensive blueprint remains elusive (Dasgupta et al., 2019; Sedrati et al., 2023). The key takeaways from following IoT governance frameworks are shown in Table 4.

Table 4. Key Takeaways from IoT Governance Frameworks

Framework	IoT-specific capabilities	Gap filled vs. COBIT/ITIL	Why it matters
IoT-Gov (Sedrati et al., 2023)	Includes five IoT governance grounds (accountability, legitimacy, roles, transparency, rules); maps duties onto a four-layer reference architecture; embeds processes for device lifecycle, data governance and security.	Adds transparency, device-centric decision-making and explicit architecture mapping missing in generic IT frameworks.	Prevents governance blind spots when autonomous devices are deployed by aligning policy, technology and stakeholder duties from strategy to field.
4I Data-Governance (Dasgupta et al., 2019)	Iterative Identify-Insulate-Inspect-Improve cycle spans full data life-cycle, consent management and continuous risk monitoring.	Provides fine-grained data protection, consent handling and real-time auditing absent in classical IT controls.	Embeds privacy-by-design for sensitive sensor data streams such as healthcare wearables.
IoT Smart-City Framework (Theodoridis et al., 2013)	Three-tier (sensor, gateway, cloud) architecture with infrastructure, experimentation and service-management planes for large-scale deployments.	Supplies guidance on edge–cloud partitioning, device discovery and real-time orchestration missing in IT governance.	Supports onboarding and performance isolation for thousands of heterogeneous urban IoT nodes.
Multi-Agent IoT Governance Architecture (Copie et al., 2013)	Distributed agents for governance-management, security-management, audit and policy enforcement with scalable autonomy.	Enables autonomous policy agents and peer-to-peer auditing not prescribed by centralized IT frameworks.	Moves policy execution close to devices, reducing latency and enabling local recovery in massive, intermittent networks.

2.5.1.1 IoT-Gov

Sedrati et al. (2023) present IoT-Gov as a layered, process-driven framework that embeds “governance by design” into every stage of an IoT system’s life cycle. Three layers (Strategic Objectives, Design & Modelling, Implementation) ensure that ethical principles, stakeholder roles, and technical choices are locked together from the outset. Five iterative processes, identify needs, assess decision-making ability, design the architecture and governance model, implement and deploy, evaluate and monitor, operationalize classic governance grounds such as accountability and

transparency while covering reference architecture, device management, data governance, and security in equal depth.

2.5.1.2 4I Data-Governance Framework

The 4I model by Dasgupta, Gill, and Hussain (2019) targets data governance inside IoT-enabled digital ecosystems. Its four phases trace a continuous loop: Identify regulatory duties and risks, insulate data through preventive controls, inspect via real-time monitoring and auditing, and improve policies considering findings. Although technology-agnostic, the framework excels at aligning GDPR, HIPAA, and similar mandates with practical controls, making it valuable wherever patient data or other sensitive streams dominate. Device lifecycle or architectural governance, however, remains out of scope.

2.5.1.3 IoT Smart-City Framework

Theodoridis et al. devised their Smart-City architecture within the EU Smart Santander project. A logical three-tier stack (sensor nodes, gateways, cloud servers) and three management planes (infrastructure, experimentation, service) enable urban services such as parking, environmental sensing, and participatory data collection. While the framework demonstrates large-scale feasibility and highlights the need for middleware, semantics, and big-data pipelines, it treats governance implicitly, noting outstanding privacy challenges and the absence of formal decision-making processes (Theodoridis et al., 2013).

2.5.1.4 Multi-Agent IoT Governance Architecture

Extending cloud-governance concepts, Copie et al. (2013) sketch a distributed, multi-agent architecture in which specialized agents, Governance-Management, Security-Management, Audit, Monitoring, Aggregation, etc., share responsibility for policy enforcement, data aggregation, and access control. By localizing decisions near devices and services, the approach promises scalability and fault-tolerance while keeping audit trails intact. Yet it remains a conceptual template; concrete tooling and metrics for accountability or transparency are still under-developed.

2.5.2 IoT Reference Architectures

The Internet of Things (IoT) is inherently complex and heterogeneous, making the development of IoT-based healthcare applications particularly challenging. Issues such as interoperability, availability, security, and privacy must be carefully addressed to ensure reliable and efficient IoT systems. One effective way to tackle these challenges is to use a reference architecture. Reference architectures provide structured frameworks that guide the design and implementation of IoT solutions, promoting standardization, scalability, and security (Barroca Filho & De Aquino Junior, 2018).

However, there is no single standardized IoT reference architecture that can address all challenges across different domains. Instead, various IoT reference architectures have been developed by companies and organizations to cater to specific industries and use cases. Some of the most notable reference architectures include the IoT-A Architecture Reference Model, ITU-T Reference Architecture, and Cisco Internet of Things Reference Model. These architectures differ in their design principles, scope, and application areas, making it essential to choose or combine the most suitable models based on the requirements of a given IoT implementation.

Table 5 provides an overview of these IoT reference architectures, highlighting their key characteristics.

Table 5. IoT Reference Architectures

Reference Architecture	Last Published	Layers	Addressed Challenges	Notes
IoT-A – Architecture Reference Model (ARM) (Bauer et al., 2013)	2013	Communication; Virtual Entity; IoT Service & Service Organization; IoT Process Management; Security; Management	Availability; Interoperability; Security and Privacy; Performance; Scalability; Trust	Comprehensive framework offering a structured, holistic approach, although its complexity may hinder understanding.
ISO/IEC 30141 Internet of Things (IoT) – Reference Architecture	2024	Foundational; Business; Usage; Functional; Trustworthiness; Construction views–viewpoints	Availability; Interoperability; Security and Privacy; Scalability; Trust; Compliance+	Provides a systematic, trustworthiness-driven approach and serves as an industry standard for IoT architectures.
IEEE Standard for an Architectural Framework for the Internet of Things (IoT) IEEE Std 2413™-2019	2019	Conceptual framework organized by multiple viewpoints (Business, Usage, Functional, Operational)	Interoperability; Security and Privacy; Scalability; Trust; Performance; Compliance	Offers a non-prescriptive, high-level framework intended to unify diverse IoT systems through common architectural principles.
ITU-T Reference Architecture	2012	Device; Network; Service and Application Support; Application; Management; Security	Interoperability; Scalability; Security and Privacy; Reliability; Performance	Developed by ITU-T to support global telecommunications and IoT deployments, it emphasizes end-to-end connectivity.
Cisco Internet of Things Reference Model	2014	Physical Devices & Controllers; Connectivity; Edge/Fog Computing; Data Accumulation; Data Abstraction; Application; Collaboration & Process	Availability; Interoperability; Security and Privacy; Performance; Scalability	Although initially developed by Cisco, this model later inspired the Industrial Internet of Things (IIRA) for industrial applications.
The Industrial Internet of Things Volume G1: Reference Architecture (IIRA) v1.9	2019	Devices; Connectivity; Edge/Fog; Data Management; Application; Business	Availability; Interoperability; Security and Privacy; Performance; Scalability	A service-oriented architecture tailored for industrial IoT, emphasizing robust connectivity and data management.
RAMI 4.0 Reference Architectural Model for Industrie 4.0	2019	Asset; Integration; Communication; Information/Data; Functional; Business	Availability; Interoperability; Security and Privacy; Performance; Scalability	A service-oriented model that supports multiple perspectives (hierarchy levels, life cycle value stream, layers) and is specialized for Industry 4.0.

2.6 Healthcare IoT-related standards and regulations

The rapid expansion of connected medical devices means that health data now flows continuously between patients, clinicians, cloud platforms, and analytic engines. This ubiquity of IoT technology magnifies longstanding concerns about confidentiality, integrity, and availability of protected information while adding new risks that arise from remote control of physical devices and unprecedented volumes of real-time

data. Three instruments dominate the current regulatory landscape for organizations that design, deploy, or manage healthcare IoT systems: the U.S. Health Insurance Portability and Accountability Act (HIPAA), the European Union's General Data Protection Regulation (GDPR), and the U.S. National Institute of Standards and Technology Interagency Report 8228 (NISTIR 8228).

2.6.1 The Health Insurance Portability and Accountability Act(HIPAA)

The Health Insurance Portability and Accountability Act of 1996 established the first comprehensive U.S. baseline for protecting individually identifiable health information and standardizing its electronic exchange (St. Cyr, 2013). In the IoT era, HIPAA is pivotal because wearable sensors, smart infusion pumps, and tele-monitoring platforms all produce protected health information(PHI); any covered entity or business associate that stores or transmits such data falls within its scope.

Key features relevant to healthcare IoT include the Privacy Rule, which governs the permissible uses and disclosures of PHI, the Security Rule, which mandates administrative, physical, and technical safeguards, and the Breach Notification Rule, which requires disclosure of incidents within sixty days. Beyond confidentiality, the statute also requires integrity and availability controls, recognizing that corrupted or inaccessible device data can compromise patient safety (Mercuri, 2004).

Compliance in an IoT setting hinges on risk-based implementation of the Security Rule's safeguards. Organizations must inventory connected devices that create or receive PHI, assess threats such as unauthorized remote access or ransomware, assign clear workforce roles, and document policies for encryption, audit logging, contingency planning, and periodic evaluation. A phased deployment

is often recommended so that staff can adapt practices while remaining alert to noncompliance gaps (Mercuri, 2004). The HITECH amendments reinforce this approach by strengthening enforcement and tying incentive payments to demonstrable security of electronic PHI.

2.6.2 GDPR - The General Data Protection Regulation

The General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, is a comprehensive legislative framework from the European Union that extends beyond EU borders, impacting any entity handling personal data of EU residents. Given that many connected medical devices capture identifiable physiological data, GDPR plays a particularly significant role in regulating healthcare IoT systems (Pulkkis et al., 2017). Its significance lies in mandating privacy by design and by default within system development, promoting principles such as data minimization, purpose specificity, user transparency, and the requirement for informed consent. The regulation also differentiates between data controllers and processors, restricts international data transfers, and enforces strict penalties that can reach up to €20 million or 4% of a company's annual global revenue(Kammueller, 2018).

Core features influencing IoT projects include requirements to conduct Data Protection Impact Assessments when technologies entail high risk, uphold data-subject rights of access, rectification, erasure, portability, and objection, and notify supervisory authorities of breaches within seventy-two hours (Pulkkis et al., 2017).

Compliance demands early integration of GDPR principles into device and service lifecycles. Developers must collect only data necessary for clinical functions, embed consent capture in user interfaces, apply strong pseudonymization or

encryption during transmission and storage, and maintain detailed processing records. Where monitoring involves sensitive biometric or behavioral patterns, organizations should appoint a data protection officer and regularly audit suppliers for adherence to contractual data-protection clauses.

2.6.3 NISTIR 8228

NISTIR 8228 is not a law but a seminal guidance document that helps organizations understand and manage cybersecurity and privacy risks associated with IoT devices across their lifecycles (Boeckl et al., 2019). It is crucial for healthcare because it translates abstract regulatory duties into concrete engineering and governance practices tailored to the unique properties of connected sensors, actuators, and gateways. The report identifies three overarching goals: protect device security, protect data security, and protect individuals' privacy, and maps each to specific risk-mitigation areas such as access management, information-flow control, and breach detection. It highlights challenges that arise when devices cannot be centrally patched, when third-party cloud services influence risk, or when sensors interact directly with the physical world (General Data Protection Regulation (GDPR) – Legal Text, 2025).

Compliance with NISTIR 8228 in a healthcare context involves extending existing enterprise risk-management processes to identify IoT assets, characterize their capabilities, and evaluate context-specific threats such as incorrect dosage delivery by a compromised pump. Organizations are urged to adjust policies, supply-chain controls, and incident-response playbooks so that they explicitly account for IoT attributes, then implement and continuously review technical safeguards consonant with HIPAA and GDPR obligations.

2.7 Toward a dedicated healthcare IoT governance framework

In sum, traditional IT governance frameworks such as ITIL, COBIT, and the ISO 27000 series remain indispensable for controlling enterprise applications and data, yet they presuppose centrally managed assets, stable trust boundaries, and human-driven workflows. They therefore leave critical IoT questions, device identity, over-the-air patching, edge autonomy, and the continuous fusion of cyber and physical risks largely unaddressed (Sedrati et al., 2023). Recent IoT-specific frameworks close many of these gaps by adding layers, processes, and reference architectures tailored to heterogeneous sensors and real-time data streams, but they are still sector-agnostic. They rarely incorporate the stringent safety, clinical effectiveness, and multi-jurisdictional privacy duties that define the healthcare context, nor do they align in detail with HIPAA, GDPR, or medical device regulations (Dasgupta et al., 2019). Consequently, neither class of framework can, on its own, guarantee that connected medical devices will remain secure, interoperable, and clinically trustworthy throughout their lifecycle; a dedicated healthcare IoT governance model is required to integrate the technical depth of IoT frameworks with the patient-centric, regulatory, and ethical imperatives of healthcare.

CHAPTER 3

METHODOLOGY

This study adopted a sequential explanatory mixed-methods design (Ivankova et al., 2006) combining a structured review of published literature with qualitative interviews to provide a deeper and more comprehensive understanding of governance challenges in healthcare IoT. In this design, the research is conducted in two distinct phases: the first phase conducts an SLR that maps and organizes existing evidence, while the second phase uses qualitative methods to further explain, elaborate on, or expand those findings. The integration of both phases takes place during the interpretation stage. This approach is particularly useful when researchers aim to validate and deepen initial results by incorporating the perspectives of individuals who experience the phenomenon in practice (Creswell & Plano Clark, 2018). It further allows the second phase to explore new areas not fully addressed in the first phase. Figure 3 shows the two-phase research process used in this study.

In Phase 1, this study adopted the systematic procedure outlined by Niknejad et al. (2020). A systematic literature review was conducted following the three-phase "planning–conducting–reporting" framework proposed by Kitchenham and Charters (Kitchenham & Charters, 2007) . To ensure a comprehensive coverage for the review, two major databases, SCOPUS (Boyle & Sherman, 2006) and Web of Science (Birkle et al., 2020) are selected for the search as they are known to be very comprehensive databases. A total of 76 studies were included and analyzed. Thirteen common governance challenges were identified and coded to show how often they appeared. This phase provided structured, evidence-based answers to RQ1 and part of RQ2.

In Phase 2, a complementary seven semi-structured interviews were carried out with experienced healthcare IoT professionals, including hospital IT leaders and vendors to complement, challenge and contextualize the published evidence with real-world experience of IoT governance, a complementary seven semi-structured interviews were carried out with experienced healthcare IoT professionals, including hospital IT leaders and vendors. The interview questions allowed participants to introduce new challenges based on their practical experience. This phase was aimed at both explaining findings from the literature and exploring issues that were not covered in existing studies. The interview data were analyzed using Braun and Clarke's (2006) six-step thematic analysis.

The two phases were carried out separately and only brought together during the interpretation stage. Several joint display tables were created to compare the literature themes with the interview findings side by side. To strengthen the interpretation of the SLR results, interview excerpts were directly linked to specific findings from the literature. Where interviewees confirmed a theme found in the SLR (e.g., critical role of data interoperability), these excerpts were used to support the literature-based analysis. Combining these two sources of evidence, published research and real-world experience, helped inform the development of a practical governance framework for healthcare IoT. This design allowed the study to use the strengths of both approaches while also expanding the scope of understanding beyond what is available in the literature.

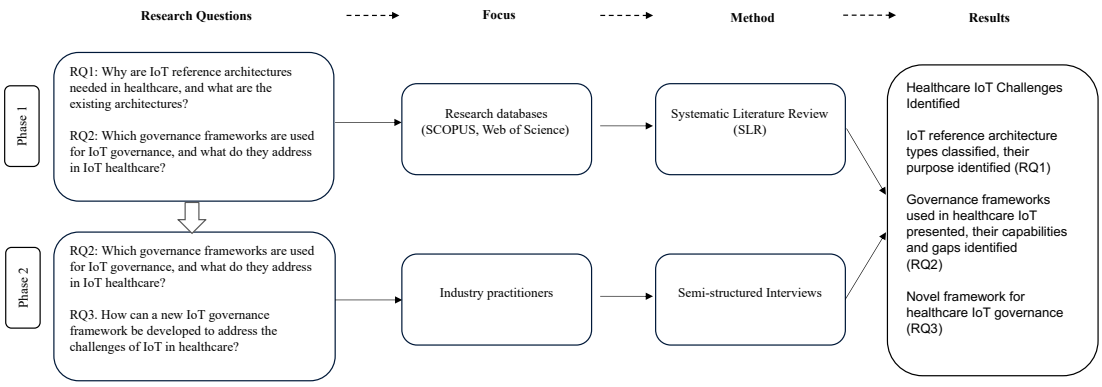

Figure 3. Research procedure

3.1 Research philosophy

The next two subsections establish the philosophical foundations that guide this study's design and analysis. First, the ontological discussion specifies what kinds of phenomena count as real within the Internet of Things (IoT) healthcare domain. Second, the epistemological discussion explains how credible claims about those phenomena can be produced within an interpretivist paradigm. By combining a social-constructionist ontology with interpretivist epistemology, the study keeps its qualitative methods coherent with the foundational view that reality is socially produced and that knowledge emerges from understanding the meanings actors attach to their practices (Berger & Luckmann, 1966; Orlikowski & Baroudi, 1991).

3.1.1 Ontology

Guided by social constructionism (Berger & Luckmann, 1966), the thesis sees IoT reference architectures, governance frameworks, and organizational routines in healthcare as socio-technical artefacts that gain reality because clinicians, patients, engineers, administrators, and regulators continuously enact, negotiate, and legitimize them in practice. Their form and influence are therefore contingent on the

meanings those actors ascribe to concepts like “secure data flow” or “clinical interoperability,” and can shift when interpretations or institutional contexts change (Orlikowski & Baroudi, 1991). This position steers the inquiry toward three questions. RQ 1 examines how stakeholders construct both the need for dedicated healthcare architectures and the specific forms those architectures take. RQ 2 explores how existing governance frameworks symbolize risk, authority, and accountability. RQ 3 assumes that a revised framework can be co-created through deliberation, because constructions are open to renegotiation when new challenges appear.

3.1.2 Epistemology

Consistent with the constructionist ontology, the study adopts an interpretivist epistemology that seeks knowledge through the reconstruction of stakeholders’ subjective and inter-subjective meanings (Klein & Myers, 1999).Validity rests on reflexivity, thick description, and credibility to participants rather than on statistical generalization (Lincoln & Guba, 1985).The systematic literature review is conducted as an interpretive synthesis of published texts that present diverse social constructions of architectures, challenges, and governance. The semi-structured interviews, analyzed thematically, elicit first-hand accounts of how healthcare actors enact and contest IoT governance. Integrating insights from both strands will produce a multi-voiced understanding that can guide the design of a governance framework that reflects the lived meanings of its intended users.

3.2 Research approach

Grounded in a social-constructionist ontology and interpretivist epistemology, this study adopted a sequential explanatory mixed-methods design (Ivankova et al., 2006) combining two qualitative strands: a systematic literature review and qualitative interviews. These are carried out independently and integrated only during interpretation, allowing published and lived constructions of healthcare IoT governance to be compared without assuming a single fixed reality.

To answer research questions in this study, the systematic approach adopted by Niknejad et al.(2020) is followed. A systematic literature review, as defined by Kitchenham and Charters (2007), is a structured method for locating, assessing, and synthesizing existing research on a particular question or topic. Researchers employ systematic literature review to consolidate current knowledge about how a technology functions and the challenges it faces, to identify gaps that prior studies have not explored, and to provide a comprehensive foundation for future work. The Kitchenham and Charters' (2007) framework organizes SLR into three sequential phases: planning, conducting, and reporting. Each phase involves tasks such as defining research questions, developing a review protocol, setting inclusion and exclusion criteria, selecting studies through a search strategy, extracting and analyzing data, and writing the report. These phases are outlined in the sections that follow.

In addition to the systematic literature review, a qualitative design was adopted that centered on seven purposively sampled, semi-structured interviews with hospital IT leaders, biomedical engineers, and senior managers from healthcare-IoT vendors, each with 5–15 years of experience. Conducted remotely via video conferencing (Google Meet), the 45 to 60-minute sessions examined challenges,

existing governance frameworks and standards, and ideal frameworks and standards attributes of a future framework. Thematic analysis was employed based on Braun and Clarke's (2006) six-phase framework. This began with data familiarization through repeated transcript reading, followed by the generation of initial codes representing key ideas across the dataset.

After each phase is analyzed separately, the two sets of findings are integrated through a joint display that places themes from the literature and themes from the interviews side by side, enabling systematic case-by-case comparison. This visual matrix allows the researcher to identify where the strands converge, thereby strengthening confidence in shared themes, and where they diverge, prompting reflection on contextual factors such as organizational culture, regulatory maturity, and technology readiness. Although the detailed outcomes for RQ1 and RQ2 will be presented in the subsequent findings and discussion chapters, the joint display serves as a methodological bridge, ensuring that insights from each strand inform the final interpretation and the development of the proposed IoT-healthcare governance framework.

3.2.1 Systematic literature review design

The sections that follow explain, in turn, how the protocol was developed, how inclusion and exclusion criteria were chosen to capture work published between 2013 and 2024, how search strings were constructed and applied across the Scopus and Web of Science databases, and how initial results were screened and filtered to arrive at the final corpus of seventy-six studies. Together, these procedures establish a transparent chain of evidence that links the research questions to the studies analyzed.

3.2.1.1 Review protocol

Once the research questions are established, the next essential stage in a systematic literature review is to design a review protocol and determine the methods that will guide the review process. This helps to reduce potential bias from the researcher (Kitchenham, 2004). In this research, the systematic literature review was carried out by following the widely accepted structure suggested by Kitchenham and Charters (2007), and the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Page et al., 2021) method was used for the systematic review. The specific steps followed in applying this framework to the current study are illustrated in Figure 4.

3.2.1.2 Inclusion and exclusion criteria

Researchers often apply inclusion and exclusion criteria to help determine whether selected articles are aligned with the objectives of the review. In this study, the primary aim is to examine the key challenges in governing healthcare IoT systems and to evaluate how existing governance frameworks address these challenges. To ensure the relevance and currency of the selected literature, this review focuses on articles published in English between 2013 and 2024. The year 2013 was selected as the starting point for the review because it marks the introduction of the Internet of Medical Things (IoMT) concept by Hu et al.(2013), which represents a key milestone in the formalization of IoT applications in healthcare. Additionally, preliminary searches indicated that peer-reviewed publications specifically addressing IoT in healthcare before 2013 were extremely limited or virtually nonexistent, further justifying this cut-off point for capturing recent and relevant developments. Over the last decade, both the technological landscape and policy

environment around healthcare IoT have evolved significantly, making earlier studies less applicable to today's context. The inclusion and exclusion criteria used for this review are summarized in Table 6.

Table 6. Research Inclusion and Exclusion Criteria

Criteria	Principle
Inclusion	Papers published between 2013 and 2024 Papers in English Full text availability Peer-reviewed studies Papers related to IoT Document Type: Conference Paper, Article, Book Chapter, Review, Book
Exclusion	Reason 1: Paper out of scope of IoT-governance-healthcare Reason 2: Paper lacks relevance to engineering or information technology disciplines.

3.2.1.3 Search strategy

As part of creating the search strategy for this study, ten keywords and their related terms were identified based on the main concepts of the research. The core terms included Internet of Things, reference architecture, healthcare, governance, and framework. For each of these, relevant synonyms were also considered. For example, in addition to "Internet of Things," the terms "IoT" and "IoMT" were used. For the healthcare domain, terms like smart healthcare, remote health, and e-health were added. These keywords were combined in different ways and tested in Google Scholar to improve the effectiveness of the search. After several trials, two final search strings were created. These search strings are shown in Table 7. The results obtained from each search string are listed in Table 8.

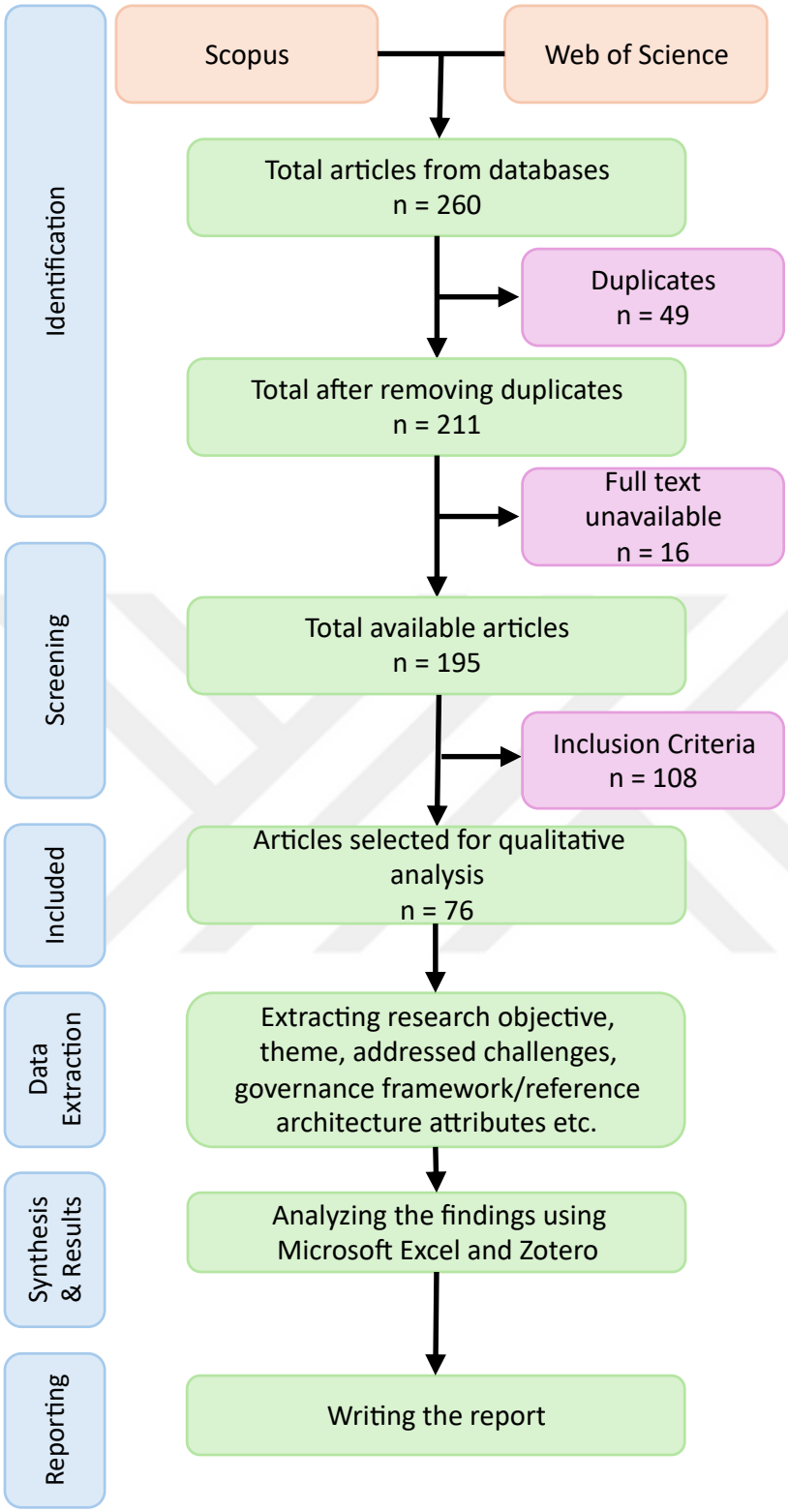

Figure 4. Application of the PRISMA review protocol

3.2.1.4 Study selection process

Using the search strategy described earlier, a total of 260 relevant papers were identified. After removing duplicate entries and papers without accessible full texts, 195 papers remained for the initial screening, which was carried out based on their titles, abstracts, and keywords. From this group, 108 papers were excluded because they did not meet the inclusion and exclusion criteria. The remaining 87 papers underwent a thorough full-text review. Following this step, 11 more papers were removed for not aligning with the set criteria. As a result, 76 studies were selected as the final primary sources, which can be seen in APPENDIX A.

Table 7. Research Questions, Search Strings, and the Importance of Questions

Research question	Search string	Importance of question
RQ1. Why are IoT reference architectures needed in healthcare, and what are the existing architecture types?	("Internet of Things" OR "iot" OR "IoMT") AND ("reference architecture" OR "reference model" OR "architectural framework" OR "model architecture") AND ("Healthcare" OR "smart hospital" OR "remote health" OR "e-health")	Understanding existing IoT reference architectures is essential to standardize practices and ensure interoperability, security, and efficient healthcare service delivery.
RQ2. Which governance frameworks are used for IoT governance, and what do they address in IoT healthcare?	("Internet of Things" OR "iot" OR "IoMT") AND ("Healthcare" OR "s mart hospital" OR "remote health" OR "e-health") AND ("governance") AND (" framework")	Evaluating current IoT governance frameworks helps highlight their effectiveness and reveal specific gaps in addressing healthcare IoT challenges.
RQ3. How can a new IoT governance framework be developed to address the challenges of IoT in healthcare?		Developing a tailored IoT governance framework provides strategic guidance and comprehensive solutions to directly mitigate identified healthcare-specific IoT challenges.

Table 8. Database Search Results for each Search String

Search String	Database	No Exclusion	Year: 2013-2024, Language: English, Document Type: Conference Paper + Article + Book Chapter + Review + Book
("Internet of Things" OR "iot" OR "IoMT") AND ("reference architecture" OR "reference model" OR "architectural framework" OR "model architecture") AND ("Healthcare" OR "smart hospital" OR "remote health" OR "e-health")	Scopus	136	124
	Web of Science	59	57
("Internet of Things" OR "iot" OR "IoMT") AND ("Healthcare" OR "smart hospital" OR "remote health" OR "e-health") AND ("governance") AND ("framework")	Scopus	64	51
	Web of Science	30	28

3.2.1.5 Data extraction overview

A three-stage workflow captured all information needed to address the research questions. In the first stage, bibliographic records were exported from Scopus and Web of Science and imported into Zotero, where each study received a unique identifier. In the second stage, every full text was read line-by-line; sentences concerning governance, architecture, challenges, or solutions were highlighted and copied to an Excel workbook, where they were open-coded following Braun and Clarke's (2006) procedure. In stage three, those codes were mapped to structured variables such as challenge category, architecture type, and how addressed, forming the dataset used for synthesis. Further details about thematic analysis are presented in Chapter 4.

3.2.1.6 Synthesis overview

The systematic literature review employed three complementary analyses to generate the findings reported in Chapter 5. Cross-tabulations mapped each reference-

architecture type and each governance framework against thirteen recurring challenge categories, yielding frequency counts that highlight where research effort has been concentrated.

3.2.2 Qualitative interview design

The qualitative interview design is introduced in four linked subsections. The first subsection outlines the sampling and recruitment strategy used to enlist participants with direct experience of healthcare IoT projects. The second explains how the semi-structured interview protocol was developed, refined, and piloted to elicit rich, context-specific accounts of governance challenges. The third describes the data collection procedures, including consent, interview logistics, recording, and transcription. The fourth provides a concise overview of the data extraction steps that prepare transcripts for coding and thematic analysis.

3.2.2.1 Sampling and recruitment

Sampling targeted the two principal environments in healthcare IoT: provider organizations that deploy and manage connected devices and technology vendors that design, build, and support them. Capturing both user-side implementation experience and developer-side constraints required purposive selection of participants with direct, hands-on involvement in IoT projects. A purposive sampling strategy was used to select participants with direct experience in IoT-enabled healthcare projects. The inclusion criterion required a minimum of five years of experience working with IoT systems in a healthcare setting, ensuring that participants had substantial practical exposure. Ultimately, seven professionals were recruited for the interview phase. These individuals represented a range of senior

technical and managerial roles, including IT project managers and directors within hospitals, as well as product managers, sales executives, and operations leaders within healthcare IoT technology providers. This composition provided a well-rounded perspective on both the deployment and development sides of IoT governance in healthcare. Interviewee roles and backgrounds are summarized in Table 9.

3.2.2.2 Interview protocol development

The interview protocol was designed to probe the full range of challenges that arise when governing IoT systems in healthcare, including security and privacy, data integration, regulatory compliance, and human-centered issues such as patient acceptance and staff resistance. Rather than addressing these areas through narrow, standalone questions, the guide employed broad prompts that encouraged participants to describe their organizations' technical workflows, operational routines, legal safeguards, and user-engagement strategies. This approach elicited rich, context-specific reflections on how diverse factors intersect in real-world deployments of healthcare IoT.

The interview phase began by establishing participants' professional background, including their roles, organizational settings, years of experience, and the types of healthcare IoT projects they had managed or supported. The subsequent questions invited them to articulate the primary challenges they encountered during the design, implementation, and operationalization of IoT solutions, and to explain how these challenges influenced project outcomes and organizational workflows. This format encouraged participants to surface the challenges they considered most pressing, whether commonly recognized or seldom discussed, as a result, deepening

the empirical understanding of IoT governance in healthcare. Particular attention was given to the role and limitations of governance frameworks. Participants were asked to comment on their use or knowledge of widely adopted models such as ISO 27001 and COBIT, and to evaluate whether these frameworks sufficiently addressed the unique risks and requirements of IoT systems in healthcare. They were encouraged to identify barriers to implementation, describe context-specific gaps, and suggest practical enhancements or new mechanisms that could strengthen governance from a governance, risk, and compliance (GRC) perspective. This open-ended, reflective structure allowed participants to reflect critical insights from their own professional experiences. The full list of interview questions is provided in APPENDIX B and APPENDIX C.

Table 9. An Overview of the Interviewee Profiles

ID	Company Type	Title	Experience in Healthcare IoT(years)
I1	Healthcare Facility Management	IT Project Manager	5.5
I2	Healthcare IoT Technology Provider	Co-Founder COO	15
I3	Healthcare IoT Technology Provider	Project Manager/ Product Manager	9
I4	Healthcare IoT Technology Provider	Director of Project Management and QA	11
I5	Healthcare IoT Technology Provider	Director of International Sales	12
I6	Healthcare IoT Technology Provider	Project Manager / Customer Success Manager	8
I7	Healthcare Facility Management	IT Director	5

3.2.2.3 Data collection procedures

Interviews were conducted remotely via video conferencing platform(Google Meet) to accommodate participants' schedules and geographical locations, ensuring flexibility and convenience. Each session lasted between 45 to 60 minutes and was guided by a semi-structured interview protocol designed to balance consistency

across interviews with the flexibility to explore emergent themes (Keen et al., 2022). Before the start of each session, participants were provided with a detailed informed consent form that explained the purpose and scope of the study, clarified the voluntary nature of their participation, outlined confidentiality safeguards, and emphasized their right to withdraw at any time without penalty.

To ensure adherence to ethical research practices, the study received formal approval from the Ethics Committee for Research Involving Humans in Social and Human Sciences (SBINAREK). The approval process involved submission of the interview protocol, informed consent documentation, and a data management plan detailing how personal information and responses would be stored and anonymized. The approval letter confirming ethical clearance is included in APPENDIX D. Only after securing this authorization, the interviews were initiated.

Each interview was both audio- and video-recorded, with participants' permission, to capture the full context of responses and non-verbal cues where possible. Recordings were transcribed verbatim shortly after each session to preserve accuracy. Transcripts were anonymized by removing personally identifiable information and assigning each participant a unique identifier corresponding to the participant profile table (see Table 9). These transcripts formed the primary data source for subsequent thematic analysis.

3.2.2.4 Data extraction overview

This study employed Braun and Clarke's (2006) six-step approach to thematic analysis to examine qualitative data collected from seven semi-structured interviews. The purpose was to identify key challenges in healthcare IoT governance, explore existing frameworks, and derive insights into the design of an ideal governance

structure. The process was systematic, iterative, and reflexive, ensuring both semantic and latent themes were considered.

In the first step, familiarization with the data, each interview transcript was read multiple times to gain a deep understanding of the content. Reflexive notes were taken to capture preliminary observations, key ideas, and potential patterns. A familiarization log was maintained to document early analytical impressions and ensure traceability across participants.

The second step involved generating initial codes. This was carried out manually using descriptive code that succinctly encapsulated the core meaning of the excerpt. All codes were derived directly from the transcripts with paraphrasing. Each code was accompanied by its corresponding verbatim quote and identified with the relevant interview ID and question number. This ensured transparency and enabled traceability during subsequent analysis stages. 237 codes were created at the end of iterations.

In the third step, the codes dataset served as the foundation for the subsequent phases of the analysis, which focused on generating, reviewing, and defining themes to identify the core challenges and governance needs in healthcare IoT implementation. The primary objective was to organize the granular initial codes into a coherent and meaningful hierarchical structure that directly addresses the research questions. The process of generating themes was both inductive and deductive. Initially, a bottom-up, inductive approach was used to develop the first level of themes, referred to here as "sub-themes." This involved carefully reviewing each initial code and its associated excerpt to understand its fundamental meaning. Codes that represented the same specific idea were grouped together under a new, more descriptive sub-theme label. For instance, initial codes such as

“staff_resistance_major_impact”, “staff_resistance_public_sector”, and “primary_challenge_staff_resistance” were all consolidated under the unifying sub-theme "Staff Resistance and Adoption Barriers". Similarly, codes like “lack_global_iot_standard” and “certification_gap_iot_rfid” were grouped into the sub-theme "Lack of Clear Standards and Certification". This initial stage transformed the raw list of codes into a more structured set of conceptual categories grounded directly in the data.

Following the creation of sub-themes, the analysis shifted to a more interpretive level to construct broader themes and overarching theme-areas. The generated sub-themes were examined for relationships and patterns, grouping related concepts into higher-order themes. For example, sub-themes such as "Staff Resistance and Adoption Barriers" and "Deficiencies in Stakeholder Knowledge" were grouped into the theme "Human and Organizational Factors," as they both relate to the people and process elements of implementation. In parallel, a deductive lens was applied by aligning these emerging themes with the research objectives. This led to the creation of three primary theme areas: "Implementation Challenges in Healthcare IoT," "Governance, Risk, and Compliance (GRC) Landscape," and "Pathways to an Improved Governance Framework." This process was iterative; themes and sub-themes were continually reviewed and refined to ensure they were distinct, internally coherent, and accurately represented the data.

The final output of this analytical process is a robust three-level thematic map that organizes all initial codes into a logical hierarchy. Each code is nested within a single sub-theme, each sub-theme belongs to one theme, and each theme is categorized under one primary theme-area, ensuring a clear and mutually exclusive structure. This systematic framework not only provides a comprehensive overview of

the challenges identified by the interviewees but also directly aligns with the research objectives, laying a solid foundation for the subsequent discussion of findings and the development of a proposed governance framework.

Overall, this thematic analysis enabled the identification of nuanced patterns and stakeholder perspectives. The structured coding and consolidation process ensured that the derived insights were both grounded in the data and organized in a way that facilitates comparison across respondents and alignment with the study's research objectives. 17 sub-themes, 7 themes, and 3 theme-areas are created. Full list of extracted themes and sub-themes shown in Table 10.

Table 10. Extracted Themes and Sub-themes from Interviews

Theme-area	Theme	Sub-theme	Sub-theme excerpt frequency
Governance, Risk, and Compliance (GRC) Landscape	Inadequacy of Existing Standards and Frameworks	Compliance as a 'Box-Ticking' Exercise	13
Governance, Risk, and Compliance (GRC) Landscape	Inadequacy of Existing Standards and Frameworks	Gaps in Technical and Security Regulations	14
Governance, Risk, and Compliance (GRC) Landscape	Inadequacy of Existing Standards and Frameworks	Limited Applicability of Current Regulations to IoT	23
Governance, Risk, and Compliance (GRC) Landscape	Pervasive Security and Privacy Vulnerabilities	Data Privacy and Compliance Concerns (KVKK, GDPR)	12
Governance, Risk, and Compliance (GRC) Landscape	Pervasive Security and Privacy Vulnerabilities	Device and Network Security Risks	13
Implementation Challenges in Healthcare IoT	Human and Organizational Factors	Deficiencies in Stakeholder Knowledge and Maturity	21
Implementation Challenges in Healthcare IoT	Human and Organizational Factors	Human and Organizational Factors (Holistic Impact)	7
Implementation Challenges in Healthcare IoT	Human and Organizational Factors	Misalignment in Project Management and Processes	22
Implementation Challenges in Healthcare IoT	Human and Organizational Factors	Staff Resistance and Adoption Barriers	22
Implementation Challenges in Healthcare IoT	Technological and Contextual Complexities	Environmental and Contextual Constraints	9
Implementation Challenges in Healthcare IoT	Technological and Contextual Complexities	Lack of Clear Standards and Certification	8
Implementation Challenges in Healthcare IoT	Technological and Contextual Complexities	Technical Implementation and Interoperability Issues	7
Implementation Challenges in Healthcare IoT	Technological and Contextual Complexities	Use Cases and Benefits of Healthcare IoT	10
Implementation Challenges in healthcare IoT	Human and Organizational Factors	Misalignment in Project Management and Processes	1
Pathways to an Improved Governance Framework	Establishing Fit-for-Purpose Standards and Processes	Call for New IoT-Specific Standards and Certification	25
Pathways to an Improved Governance Framework	Fostering a Culture of Governance and Awareness	Enhancing Stakeholder Education and Training	11
Pathways to an Improved Governance Framework	Fostering a Culture of Governance and Awareness	Prioritizing the Human Factor in Design and Processes	12
Pathways to an Improved Governance Framework	Pathways to an Improved Governance Framework	Improving Project Lifecycle and Management Practices	18

3.2.3 Integration plan of systematic literature review and qualitative interviews

Following separate analyses of the systematic literature review and the interview transcripts, the two strands are brought together in a joint display that aligns each of the thirteen challenge categories with the corresponding themes that emerged from practitioner accounts. The display contrasted the tiered SLR coverage scores with qualitative descriptors such as frequency and illustrative quotations. This side-by-side arrangement allows a direct comparison of evidence strength and experiential relevance, revealing points of convergence that reinforce the credibility of shared findings and areas of divergence that require contextual explanation, such as differing organizational cultures, stages of regulatory maturity or levels of technology readiness. Where both phases' findings agree, the study gains confidence that these domains are firmly established priorities. Where they diverge, the joint display signals the need to explore these gaps in the design of the governance framework.

Integration proceeds through three steps. First, numeric and thematic data are transformed into comparable ordinal categories so that both strands can be viewed on a common scale. Second, discrepancies are examined with reference to interview context notes to determine whether they stem from sectoral differences or methodological limitations in the literature. Third, the combined evidence is synthesized into meta-inferences that guide the selection of control domains and mechanisms for the proposed framework. This integrative procedure ensures that the final governance model addresses empirically validated strengths while incorporating practitioner-endorsed solutions for under-governed areas. Detailed integrative findings and their implications are presented in Chapter 5.

CHAPTER 4

DATA EXTRACTION AND SYNTHESIS

This chapter explains how two complementary evidence sets, a systematic literature review of seventy-six peer-reviewed studies and qualitative interviews with seven senior stakeholders, were transformed into rigorously coded data that anchor the thesis. The review, extracted with a custom form that logged “Governance”, “Architecture”, “Challenge”, and “Solution” was coded using Braun and Clarke’s six-phase approach. Resulting outputs include corpus profiles that show journal articles predominate, IEEE leads publisher share, and research volume peaks in 2021, plus thematic maps that identify thirteen canonical “challenge” categories headed by “Security and Privacy” and “Data Management”, five reference-architecture reference architecture types from “Three-Layer Classical” to “Standards-Aligned”, and three governance-framework clusters: “Formal IT-G standards”, “Hybrid/blockchain”, and “Sector-specific healthcare”. The interview stream contributes 248 excerpts organized into seven “themes” and seventeen “sub-themes.” Descriptive tables show “Human and Organizational Factors” and “Inadequacy of Existing Standards and Frameworks” as the most frequent themes; an “Interviewee–Theme Matrix” highlights that facility managers emphasize staff-resistance issues whereas vendors stress regulatory gaps. A “Sub-theme” co-occurrence heat map demonstrates that regulatory, procurement, and human factors often appear together in single narratives. Collectively, these frequencies, prevalence metrics and relational visualizations provide a transparent analytic platform for the interpretive synthesis in the next chapter.

4.1 Systematic literature review

This section traces how seventy-six peer-reviewed studies, retrieved from Scopus and Web of Science, inform the four research questions on IoT governance in healthcare. It begins by explaining the bespoke data-extraction form, which captured metadata and four analytic dimensions, “Governance,” “Architecture,” “Challenge,” and “Solution”, before guiding a Braun and Clarke (2006) thematic analysis across full texts imported into Zotero and coded in Excel. It then profiles the corpus, detailing document types, publisher venues, publication year trends, and methodological approaches to show both the disciplinary breadth and the pandemic-driven surge in 2021. The review proceeds to report thematic results: primary “themes” that distinguish governance frameworks from reference architectures, thirteen canonical “challenge” categories grounded in security, data management, and interoperability, and five emergent reference architecture types that range from the classical three-layer stack to standards-aligned designs. Finally, cross-tabulation matrices link the reference architecture types and governance clusters to the challenge categories. Together, these sections provide a structured, transparent map of how existing scholarship addresses IoT governance problems, thereby setting the empirical stage for comparing literature insights with the interview findings presented earlier in the chapter.

4.1.1 Data extraction form design

Each of the 76 primary studies was examined in detail, and information related to the four research questions was carefully documented. Metadata was retrieved from the Scopus and Web of Science databases.

To extract relevant data about challenges, governance frameworks, reference architectures, solutions, and gaps, thematic analysis was conducted. The six-phase approach of Braun and Clarke (2006) guided the qualitative coding, but the lens was widened to capture four analytic dimensions: Governance, Architecture, Challenge, and Solution. Full texts were first imported into Zotero (version 7.0.15). While reading, the researcher highlighted and tagged any sentence that discussed a governance arrangement, a system architecture, an explicit difficulty, or a proposed solution. Highlights were then exported into Microsoft Excel for open coding. Each row held one excerpt, a brief descriptive code and a column that marked the analytic dimension. For instance, a sentence that described a fog gateway was placed under Architecture. After the initial coding round, related labels were examined and merged.

Challenge excerpts were gathered and grouped under 13 challenge categories shown in Table 11. Their identifiers and labels were stored in Addressed Challenge Category IDs and Addressed Challenge Categories. If an excerpt described how a study proposes a solution to a challenge, such as through encryption, edge processing, etc., the summary went into how it addressed unresolved matters were entered as Remaining Gaps.

Regulatory standards and governance references were captured at the same time. Mentions of laws like HIPAA or GDPR populated Regulations Mentioned, and any explanation of how compliance was achieved was summarized in Regulation Compliance Approach. References to technical standards such as HL7 FHIR or IEEE 802.15.4e were entered under Standards Mentioned, and when relevant, Standards Implementation clarified how the standard was applied. Citations of broader IT governance models like ITIL or COBIT were put into the IT Governance

Frameworks Mentioned field, with practical details noted in the IT Governance Implementation Details.

During axial coding, we reorganized the open-coded "reference-architecture" excerpts into higher-order properties, layer count, presence of an explicit edge tier, use of service-orientation, security overlays, and adherence to formal standards. Constant comparison of those properties across the relevant 68 studies produced five coherent clusters: Three-Layer Classical, Four-Layer Edge-Oriented, Multi-Layer / Viewpoint Service-Oriented, Security-Focused, and Standards-Aligned. Each cluster shares a distinctive combination of layer structure, characteristic attributes, and illustrative papers, allowing us to treat it as an IoT reference architecture type for subsequent cross-tabulation with challenges and governance mechanisms.

For governance framework fields, first, an inductive open-coding pass was undertaken across the "Governance Framework," "Governance Framework Type," "Standards/IT-Governance Implementation," and related textual extraction fields. Keywords denoting explicit reliance on cross-industry IT-governance bodies of knowledge (e.g., COBIT 2019, ISO 27001/27799, ITIL 4, "GRC platform," "shared-responsibility model") consistently co-occurred and were provisionally labelled Formal IT-G standards. A second code family captured frameworks grounded in emerging technological enablers, most frequently blockchain, zero-trust cloud, or edge-centric smart-contract layers, yielding the Hybrid / blockchain theme. Residual instances that neither invoked formal IT-G standards nor embedded disruptive ledger/cloud primitives yet were purpose-built for clinical or organizational healthcare contexts were grouped as Sector-specific healthcare frameworks. Constant-comparison checks, and keyword refinement were iterated to all 76 records.

Finally, the four dimensions were distilled into the Theme 1 column. When a paper centered on oversight, it was labelled Governance Framework; when it focused on system structure, it became Reference Architecture. Papers that integrated both received the combined label, while purely descriptive items were set to N/A.

This integrated workflow ensured that governance frameworks, reference architectures, challenges, compliance matters, and standards were all captured in their own fields, giving a full picture of how each study contributes to IoT healthcare research.

Table 11. Healthcare IoT Challenge Categories

Challenge Id	Challenge Name
C1	Security and Privacy
C2	Data Management
C3	Interoperability/Standards
C4	Scalability
C5	Regulatory Compliance
C6	Accountability and Transparency
C7	Latency/Real-Time Performance
C8	Device Management
C9	Mobility
C10	Energy Efficiency
C11	Ethical Concerns
C12	Patient Acceptance and Awareness
C13	User Resistance and Adoption Barriers

The extracted data column names and their descriptions are presented in Table 12.

4.1.2 Corpus characteristics

The distribution of document types among the 76 primary studies included in the review. Most of the sources are journal articles (43), followed by conference papers (25), and a smaller number of book sections (8), as seen in Figure 5.

Table 12. Extracted Data from Primary Papers

Extracted Data	Description
Paper Id	A unique identifier assigned to each study
Related RQs	The research questions answered in the study
Title	Title of the study
Author/Year	Author(s) name and year of the study published
Abstract	Author-supplied abstract. “N/A” is entered if no abstract is available.
Keywords	Keywords reported by the authors, separated by semicolons; “N/A” if absent.
Objective	The main objective of the study
Research strategy	Case study, conceptual study, survey, interview, systematic literature review etc.
Methodology	Qualitative, quantitative, mixed method
Data collection method	Survey, interview, literature review, documentation, observation etc.
Subject	Data collection subjects such as interview and survey participants or papers in a literature review
Country/Region	The specific country or region that the reviewed paper focuses on
Online database/publisher	Where the paper was published
Document type	Article, conference paper, review
Journal/Conference Name	Name of the conference or journal where the paper was presented or published
Theme 1	The focus of the study reference architecture, governance framework or both.
Theme 2	Secondary or sub-theme created inductively to capture finer distinctions; “N/A” if not applicable.
Healthcare Context	Healthcare related context extracted from study. Implementation, targeted or mentioned.
Healthcare Setting Cluster	Implementation , or targeted implementation area of the study. Hospital settings, telehealth, wearable health devices, emergency care or general. N/A if not directly targeted.
Addressed Challenge Category IDs	Comma-separated list of the thirteen derived challenge category themes (C1–C13) to which the paper’s challenges were mapped.
Addressed Challenge Categories	Human-readable names that correspond to the codes in the previous column, separated by semicolons.
Specific Challenges	Paraphrased phrases that articulate the precise difficulties discussed, expressed in the authors’ wording where possible.
How Addressed	Summary of the technical or organizational remedies the study proposes for those specific challenges.
Reference Architecture	Used, proposed reference architecture in the study. N/A if not relevant.
Reference Architecture Type	Broader category of Reference Architectures. Includes 5 values. N/A if not relevant.
Governance Framework	Used, proposed governance framework in the study. N/A if not relevant.
Governance Framework Cluster	Broader category of Governance Frameworks. Includes 3 values. N/A if not relevant.
Remaining Gaps	Short description of unresolved issues or future work identified by the authors or by the coder.
Validation/Evaluation	Type of assessment carried out, such as “Simulation,” “Test-bed experiment,” or “Low.”
Regulations Mentioned	Laws or directives cited in the paper (HIPAA, GDPR, etc.) or “NR.”
Regulation Compliance Approach	How the authors claim to satisfy the regulations named; “N/A” if not addressed.
Standards Mentioned	Technical or clinical standards referenced (HL7 FHIR, IEEE 802.15.4e etc.) or “N/A.”
Standards Implementation	Explanation of how those standards are applied in the proposed system, if at all.
IT Governance Frameworks Mentioned	Any mainstream IT-governance models cited (COBIT, ITIL) or “NR.”
IT Governance Implementation Details	Specifics of how such frameworks are used in the study context or "N/A"
Challenge Coverage Breadth	How many challenge categories are addressed.
Evidence Weight	Derived from Validation/Evaluation and Research Strategy. Values 0.5, 1.0, 1.5, 2
Healthcare Context Weight	If healthcare implementation or direct focus is mentioned then 1, otherwise 0.7.
Composite Reliability	Evidence Weight X Healthcare Context Weight. Values between 0.35 and 2.
Weighted Challenge Coverage	Challenge Coverage Breadth X Composite Reliability

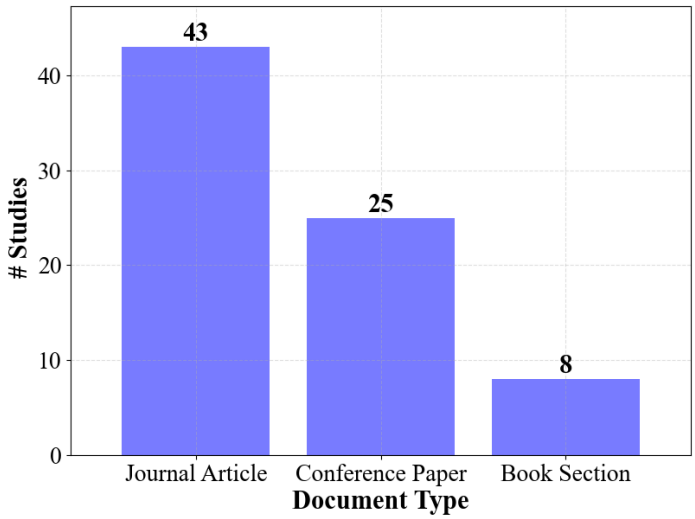

Figure 5. Distribution of primary studies based on document type

Most of the selected primary studies were published in respected academic venues, including high-impact journals and prominent conference proceedings. Most notably, a significant portion of the reviewed papers appeared in IEEE publications (25 papers), reflecting the organization's leading role in disseminating research on engineering, technology, and information systems. Springer followed closely with 15 papers, demonstrating its strong presence in multidisciplinary scientific publishing, especially in emerging technology domains like IoT and healthcare. Elsevier, known for its well-established peer-reviewed journals and platforms such as ScienceDirect, accounted for 11 studies, highlighting its relevance to health informatics and governance-related topics. MDPI, an open-access publisher gaining recognition for its rapid dissemination and thematic focus, contributed 6 papers to the final selection. Although several other publishers were represented with fewer studies, their inclusion in Scopus or Web of Science ensures the academic credibility and peer-reviewed nature of all selected works. This broad distribution underscores the interdisciplinary nature of IoT governance in healthcare and the wide interest it has generated across various research communities.

Figure 6 shows the yearly distribution of primary studies related to IoT governance in healthcare. A steady rise in research output is observed from 2014 onwards, with a noticeable peak in 2021. This increase aligns with the COVID-19 pandemic, during which there was an urgent global focus on digital health solutions, including remote monitoring, telemedicine, and IoT-enabled healthcare infrastructure. The pandemic accelerated both the deployment and academic exploration of IoT systems, especially regarding data governance, privacy, and system resilience.

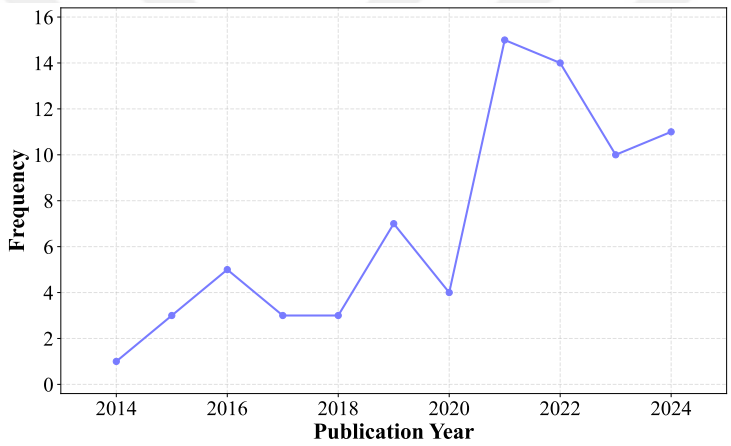

Figure 6. A temporal view of the primary studies

Although the number of publications appears to decline slightly after 2021, this should not be interpreted as a drop in relevance. Rather, 2021 represents an exceptional spike, driven by the global emergency. The post-2021 period reflects a return to typical research cycles rather than a decrease in interest or importance. The ongoing developments in healthcare digitization and regulatory adaptations continue to support steady scholarly attention to this domain.

Figure 7 shows the distribution of research strategies used across the primary studies. The most common approach was the conceptual study (29 studies),

highlighting the field's focus on theory development and framework design. A significant number of studies (22) combined conceptual work with single case studies, suggesting efforts to apply or test proposed ideas in real-world settings. Another 10 studies paired conceptual approaches with literature reviews, while smaller groups relied solely on single case studies (7) or standalone literature reviews (6). This indicates that while theoretical development remains dominant, there is growing attention toward combining it with empirical or structured review methods for greater validity.

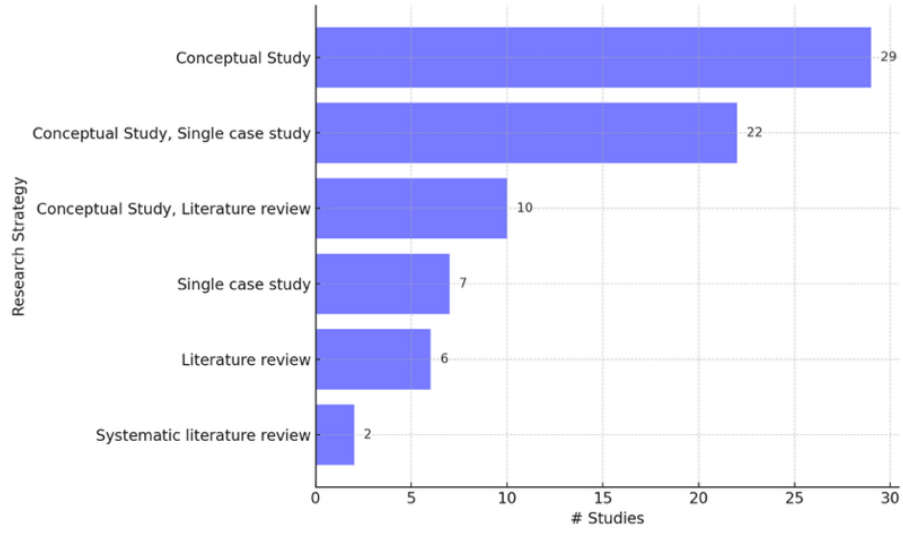

Figure 7. Distribution of research strategies

Most of these studies (48 out of 76) use qualitative methods, such as interviews or case studies, to understand how IoT is governed in healthcare. Fourteen studies combine both qualitative and quantitative approaches. Fourteen studies use a fully quantitative method with numbers and statistics.

4.1.3 Thematic analysis results

This subsection presents thematic analysis results with primary themes, challenge categories, reference architecture types and governance framework clusters extractions.

4.1.3.1 Primary themes

Table 13 organizes the seventy-six primary papers by the value recorded in the Theme 1 column of the spreadsheet. Four groups appear. Most studies, forty-four in total, fall under Reference Architecture because their main contribution is a multi-layer design or structural model. A further twenty-four papers integrate an architectural proposal with an explicit governance layer and are coded Governance Framework + Reference Architecture. Eight papers concentrate primarily on oversight models and are therefore labelled Governance Framework. Only one study, P73, lacks enough architectural or governance detail to fit these labels and remains N/A. This distribution shows that research on IoT healthcare pays greatest attention to structural designs, yet a sizeable minority of authors now combine architecture with governance elements, suggesting a trend toward integrated design-and-govern approaches.

Table 13. List of Themes, Definitions, and Related Primary Papers.

Theme	Description	Paper IDs
Governance Framework	Studies whose main contribution is a governance framework or policy model for IoT healthcare.	P3; P5; P6; P37; P38; P39; P56; P73
Reference Architecture	Studies that propose or analyze a reference architecture for IoT healthcare.	P1; P4; P7; P9; P10; P11; P14; P15; P22; P23; P25; P31; P32; P33; P34; P36; P40; P41; P42; P43; P44; P45; P46; P47; P48; P49; P52; P53; P54; P57; P58; P60; P61; P63; P64; P65; P66; P68; P69; P70; P71; P72; P74; P75
Governance Framework + Reference Architecture	Studies that combine a governance framework with a reference architecture.	P2; P8; P12; P13; P16; P17; P18; P19; P20; P21; P24; P26; P27; P28; P29; P30; P35; P50; P51; P55; P59; P62; P67; P76

4.1.3.2 Challenge categories

The thematic analysis highlights five dominant challenge categories (see Figure 8).Foremost, 64 papers (≈ 84 %) emphasize safeguarding patient information and securing connected devices, underscoring that robust security-and-privacy controls remain the most important aspect for IoT-enabled healthcare (Dang et al., 2021; Hasan et al., 2022; Mishra & Singh, 2023). Second, 58 studies (≈ 77%) foreground data-management concerns, standardized storage formats, provenance tracking, and life-cycle governance, reflecting the field's recognition that analytic reliability hinges on orderly data handling (Elgammal & Krämer, 2021; Gohar et al., 2022; Hasselgren et al., 2021). Third, 51 papers (≈ 68 %) draw attention to persistent interoperability and standard gaps; they advocate common interfaces and syntactic/semantic standards so heterogeneous sensors, platforms, and electronic health-record systems can interoperate seamlessly (Talaminos-Barroso et al., 2022; Valero et al., 2021). Fourth, 36 publications (≈ 47 %) warn that escalating device volumes and data flux threaten network or cloud bottlenecks (Akkaoui et al., 2020; Islam et al., 2023). Fifth, 30 works (≈ 39 %) expressly tackle regulatory compliance, ranging from HIPAA/GDPR alignment to sector-specific audit logging, often suggesting dedicated

compliance layers or policy engines embedded within the reference architecture (Ali et al., 2024; B. Prasad & Ramachandram, 2021). Finally, 30 papers (≈ 40 %) focus on accountability and transparency, advocating immutable audit trails, fine-grained access logs, and explainable analytics so that data provenance and algorithmic decisions remain visible to both clinicians and external auditors (Kakkar, 2019; Sulis et al., 2021). Collectively, these frequencies reveal a research agenda still dominated by classic technical and legal foundations, while comparatively fewer studies engage with softer socio-ethical challenges (e.g., user acceptance, energy efficiency), signaling fertile ground for future inquiry.

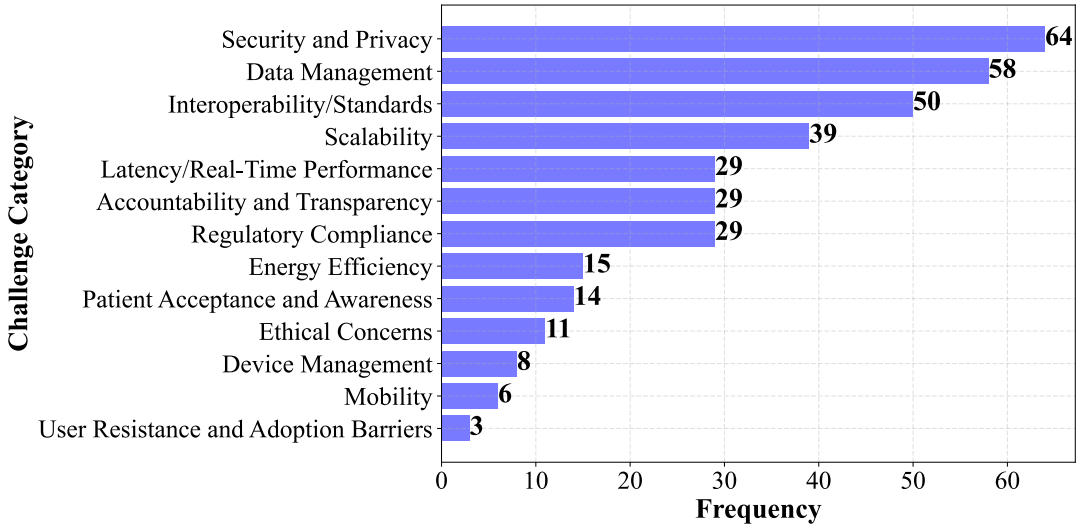

Figure 8. Frequencies of challenge categories from the SLR

4.1.3.3 Reference architecture types and governance framework clusters

Table 14 shows the five IoT reference-architecture types extracted in thematic analysis, revealing prevailing design emphases. The “Three-Layer Classical” model (n = 11) reprises the canonical perception–network–application stack common in early WBAN prototypes; although conceptually simple, its limited vertical span

affords little headroom for scalability or advanced governance mechanisms. By contrast, the “Four-Layer Edge-Oriented” reference architecture type (n = 12) inserts an explicit edge/fog tier between devices and the cloud, enabling latency-sensitive preprocessing and traffic offloading (Firouzi et al., 2022). A further elaboration appears in the “Multi-Layer / Viewpoint Service-Oriented” category (n = 12), which augments the stack with middleware and business/analytics views to facilitate service orchestration and higher-level decision support (Pir et al., 2015). The largest cluster, labelled “Security-Focused” (n = 29), overlays heterogeneous layer arrangements with cross-cutting trust technologies, blockchain, homomorphic encryption, distributed ledgers, signaling heightened concern for end-to-end credibility in data handling (Preetham et al., 2023, p. 5; Sawand et al., 2014). Finally, a smaller but distinctive “Standards-Aligned” set (n = 5) explicitly conforms to formal frameworks such as ISO/IEC 30141, IEEE 2413, or RAMI 4.0, inheriting their interoperability semantics and governance hooks (Aranha et al., 2019). Taken together, these reference architecture types trace a trajectory from minimal three-tier stacks towards richer, security- and service-aware architectures, with formal standards adoption still emerging as a niche but strategically important approach for healthcare IoT governance.

Figure 9 shows that Hybrid/blockchain proposals constitute the largest single cluster (n = 9), closely followed by Formal IT-G standards adaptations (n = 8), with bespoke healthcare models the smallest category (n = 5). This tripartite typology provides a coherent lens for subsequent challenge-coverage and reliability analyses by aligning governance propositions with their underlying normative and technological foundations.

Table 14. Healthcare IoT Reference Architectures Types

Reference Architecture Type	Layer Structure / Views	Characteristic Attributes	Representative Papers (IDs)
Three-Layer Classical	Perception / Sensing – Network – Application	Minimal three-tier stack prevalent in early WBAN prototypes; limited scalability.	P11, P12, P15, P17, P23, P43, P49, P54, P57, P58, P71
Four-Layer Edge-Oriented	Device – Edge / Fog – Cloud – Application	Edge/fog tier handles latency-sensitive tasks, reducing cloud traffic.	P4, P7, P25, P36, P40, P41, P45, P46, P64, P68, P69, P75
Multi-Layer / Viewpoint Service-Oriented	Device – Network / Edge – Middleware / Platform – Application – Business / Analytics	Adds middleware and business viewpoints; supports orchestration and analytics.	P1, P9, P27, P31, P44, P48, P52, P55, P65, P66, P67, P72
Security-Focused	Layer stack varies; security overlay (e.g., blockchain, encryption) across 3–6 layers	Introduces trust technologies (blockchain, homomorphic encryption) across layers.	P2, P8, P10, P14, P16, P18, P19, P20, P21, P22, P24, P26, P28, P29, P30, P33, P34, P35, P42, P47, P50, P53, P59, P60, P61, P63, P70, P74, P76
Standards-Aligned	Conforms to ISO/IEC 30141, IEEE 2413, RAMI 4.0, IoT-A, or similar	Inherits formal structures (IoT-A, ISO/IEC 30141, IEEE 2413) for interoperability.	P13, P32, P51, P62

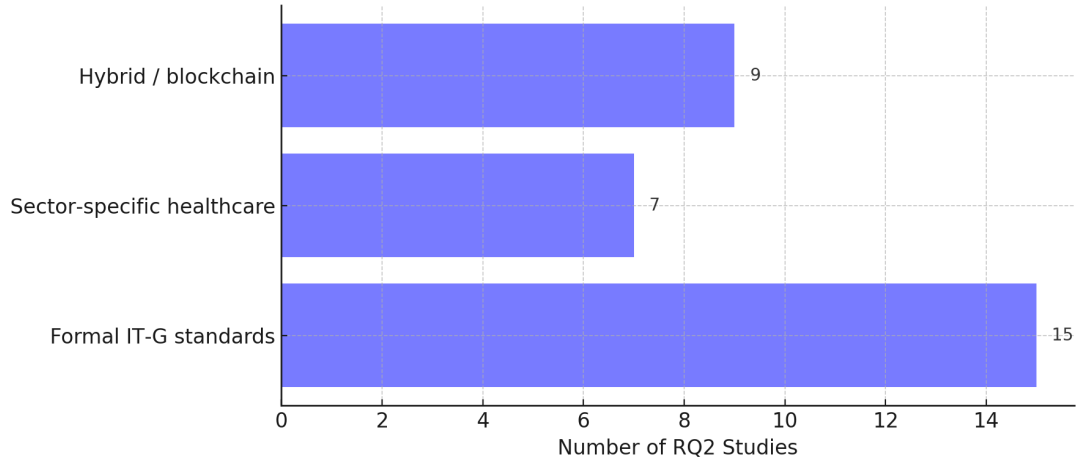

Figure 9. Distribution of governance framework clusters

4.1.4 Cross-tabulation synthesis results

This cross-tabulation section quantifies how well existing solutions confront practical hurdles by aligning the five reference-architecture types and the three governance-framework clusters with the thirteen canonical challenge categories. The

first matrix shows challenge coverage for each architecture, while the second repeats the analysis for governance models.

4.1.4.1 Reference architecture type X challenge matrices

This sub-section employs a two-pass cross-tabulation to quantify how well each reference architecture type addresses the thirteen canonical healthcare Internet of Things challenges. In the first pass, every study's "Addressed Challenge Categories" codes are exploded into individual tokens, mapped to the canonical challenge list, and grouped by the five reference architecture types introduced in Table 15.

Table 15. Challenge Coverage Counts per Reference Architecture

Challenge Category	Four-Layer Edge-Oriented	Multi-Layer / Viewpoint Service-Oriented	Security-Focused	Standards-Aligned	Three-Layer Classical
Total Paper Count	12	12	29	4	11
Security and Privacy	10	9	29	3	6
Data Management	9	10	23	3	8
Interoperability/Standards	9	12	16	2	8
Scalability	10	6	17	0	4
Regulatory Compliance	3	2	13	3	2
Accountability and Transparency	1	1	15	4	3
Latency/Real-Time Performance	7	7	9	0	3
Energy Efficiency	5	3	4	0	2
Patient Acceptance and Awareness	2	2	2	1	2
Ethical Concerns	2	1	1	1	0
Device Management	0	0	5	1	1
Mobility	1	0	1	0	1
User Resistance and Adoption Barriers	0	0	1	0	0

4.1.4.2 Governance framework and challenge category cross-tabulation

To avoid duplicating the methodological exposition already presented for the architecture analysis, the governance-framework extraction pipeline reuses its core steps while foregrounding two changes that are unique to RQ2. It uses "Governance

Framework", "Governance Framework Cluster" columns instead of "Reference Architecture Type". First, the framework's "Addressed Challenge Categories" field was exploded into the same thirteen canonical challenges and then grouped by framework identifier rather than by architecture type. As with the reference architecture type analysis, a second run is unnecessary because governance studies, by definition, already focus on RQ2.

The same analysis pipeline was used for governance framework clusters shown in Figure 9. The frequency matrix (see Table 16) shows that security and privacy dominate all clusters, appearing in more than 90% of the 32 frameworks, while data management, interoperability, and regulatory compliance constitute the next most common concerns. Accountability and transparency now surface in more than two-thirds of the frameworks, overtaking their coverage in the architectural corpus and signaling a growing emphasis on auditability. In contrast, energy efficiency, latency, mobility, and user-resistance issues remain peripheral; energy efficiency is mentioned in only one framework, and no framework explicitly addresses mobility or user resistance.

Table 16. Challenge Coverage Counts per Governance Framework Cluster

	Formal IT-G standards	Hybrid / blockchain	Sector-specific healthcare
Total Paper Count	15	9	7
Security and Privacy	13	9	6
Data Management	10	9	4
Interoperability/Standards	8	2	5
Scalability	6	5	1
Regulatory Compliance	9	4	5
Accountability and Transparency	13	6	3
Latency/Real-Time Performance	2	1	1
Energy Efficiency	1	0	0
Patient Acceptance and Awareness	0	1	2
Ethical Concerns	0	0	3
Device Management	2	1	0
Mobility	0	0	0
User Resistance and Adoption Barriers	0	0	0

4.2 Qualitative interviews

This qualitative-interview segment first grounds the reader in the data: seven senior stakeholders, including facility managers and technology-provider directors, generated 248 coded excerpts that populate seven overarching “themes” and seventeen finer-grained “sub-themes” related to Internet-of-Things governance in clinical settings. After outlining these descriptive counts, the narrative moves into cross-case exploration through three tightly linked analyses. The “Interviewee–Theme Matrix” heat map shows how excerpt volume differs by participant, highlighting, for example, which vendors emphasize “Inadequacy of Existing Standards and Frameworks”, and which facility managers focus on “Human and Organizational Factors.”. Finally, the “Co-occurrence Heat Map” uncovers how concerns about regulation, project management, and human factors cluster within the same interviewee narratives, demonstrating that governance challenges are often intertwined rather than isolated. Together, these analyses move from describing what

is in the corpus to comparing who talks about what and to what degree, providing a nuanced empirical foundation for the interpretive findings that follow.

4.2.1 Descriptives

Table 17 summarizes the scope and granularity of the qualitative dataset. Seven interviewees generated 248 excerpts, 237 distinct coding references. These codes were inductively consolidated into 17 sub-themes, themselves nested within seven themes that map onto three higher-level theme areas. The ratio of excerpts to interviewees, approximately 35% participants, and the near one-to-one correspondence between codes and excerpts indicate a rich yet disciplined coding process. This breadth of coding, coupled with multi-level thematic aggregation, provides a robust foundation for cross-case comparison and thematic synthesis in subsequent sections of the thesis.

Table 17. Descriptive Overview of the Interview Analysis

Metric	Value
Number of Interviewees	7
Theme areas	3
Themes	7
Sub-themes	17
Codes	237
Excerpts	248

Figure 10 visualizes the distribution of coded interview excerpts across the three analytic areas that scaffold this study. “Implementation Challenges in Healthcare IoT” accounts for 43% of all excerpts, highlighting its salience in participants’ accounts of daily practice. “Governance, Risk, and Compliance” contributes 30%, signaling that regulatory and oversight concerns remain central but somewhat less dominant. “Pathways to an Improved Governance Framework”

comprises the remaining 27%, showing that respondents also devoted substantial attention to prospective solutions. The relative balance among these areas suggests that the data corpus is sufficiently broad to inform each of the three research questions. Moreover, the prominence of implementation challenges indicates that any proposed governance framework must be firmly grounded in operational realities rather than confined to high-level policy discourse.

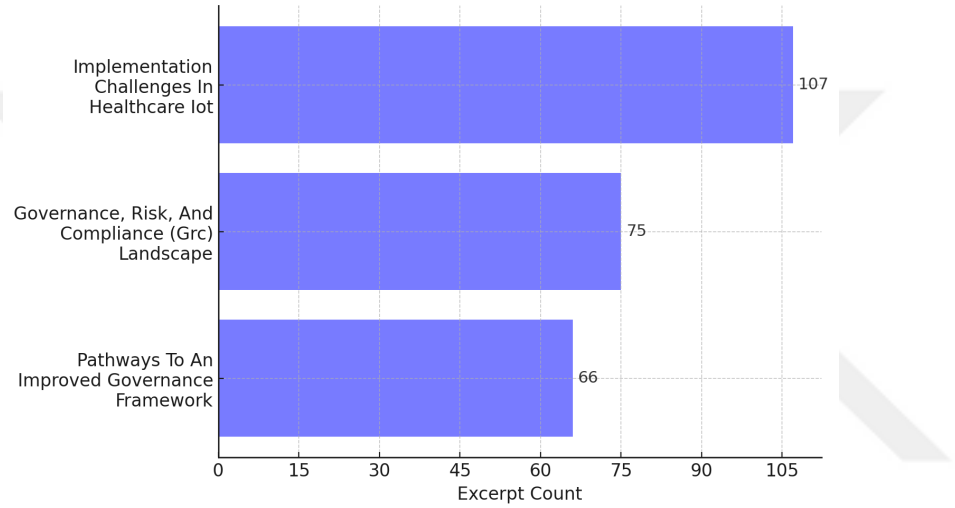

Figure 10. Excerpt count by theme area

Figure 11 shows that “Human and Organizational Factors” dominate the discourse with 73 excerpts, underscoring the prominence of staff attitudes, culture, and competencies in shaping IoT-enabled healthcare. “Inadequacy of Existing Standards and Frameworks” follows with 50, revealing widespread concern that current governance guidance remains insufficient. “Technological and Contextual Complexities” registers 34 excerpts, indicating that practical integration issues also weigh heavily on implementation efforts. The remaining four themes each attract between 18 and 25 excerpts, suggesting that although they are less frequently raised, they still contribute meaningfully to the overall narrative. Together, these

distributions confirm that the interview corpus balances operational, regulatory, and prospective considerations, thereby providing a robust basis for addressing each research question.

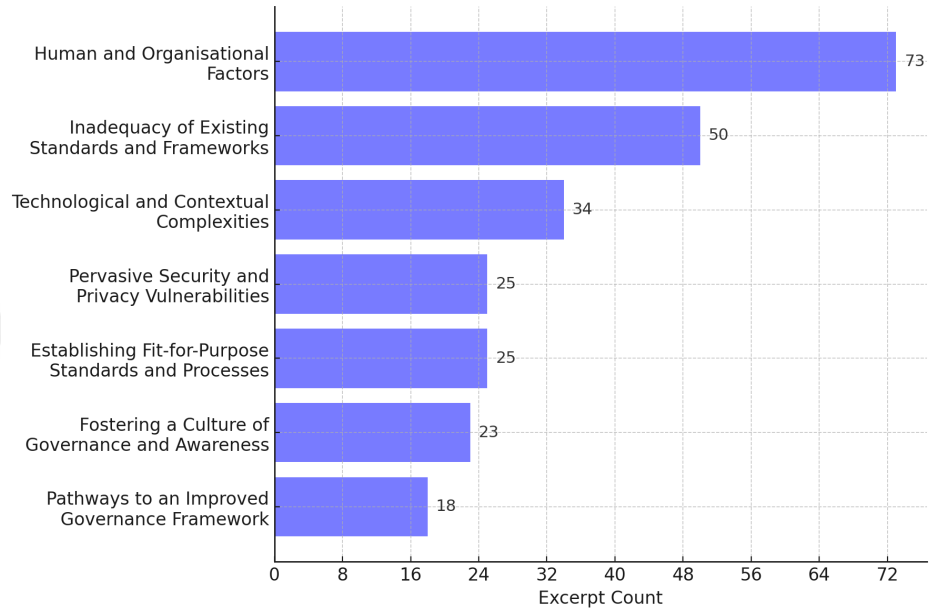

Figure 11. Excerpt count by theme

Figure 12 deepens this picture by isolating the most frequently invoked sub-topics. The leading sub-theme, “Call for New IoT-Specific Standards and Certification”, accounts for 25 excerpts, reinforcing the finding that respondents view the current regulatory landscape as incomplete. “Limited Applicability of Current Regulations to Healthcare IoT” and “Misalignment in Project Management and Processes” each attract 23 excerpts, indicating a strong perception that existing rules do not map neatly onto day-to-day project realities. “Staff Resistance and Adoption Barriers”, at 22 excerpts, highlights the human dimension of governance challenges, while “Deficiencies in Stakeholder Knowledge and Maturity”, at 21 excerpts, illustrates a persistent capability gap. The remaining sub-themes taper

gradually, yet low falls below 12 excerpts, implying that even the lower-frequency issues are not merely incidental. This long-tail distribution shows that governance concerns are multifaceted, spanning technical, managerial, and human factors, and it suggests that any proposed framework must be both comprehensive and flexible to address this breadth of issues.

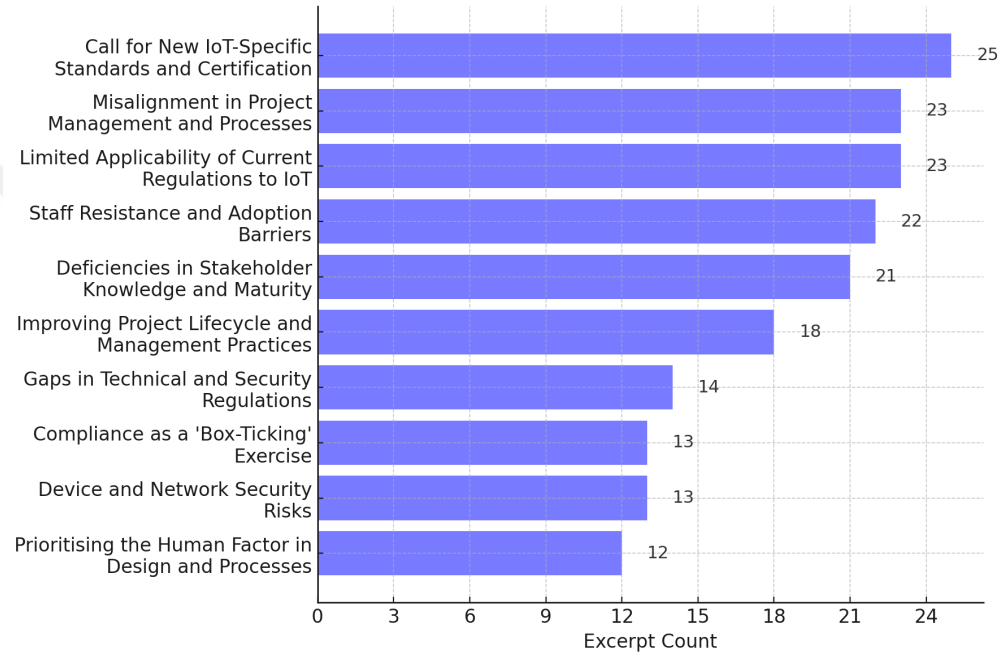

Figure 12. Excerpt count for top ten sub-themes

4.2.2 Cross-case thematic pattern analysis

Cross-case thematic pattern analysis compares how each interviewee engages with the coded themes, moving beyond overall frequencies to reveal participant-specific emphases and the intersections among sub-themes within individual narratives.

4.2.2.1 Interviewee–Theme Matrix: Excerpt Distribution

Table 18 reports the raw excerpt counts for every sub-theme across the seven interviewees. For example, Interviewee 2, the most experienced participant, allocates

more than 15% of their excerpts to Limited Applicability of Current Regulations to Healthcare IoT, whereas Interviewee 7 devotes only five percent to that sub-theme, suggesting that deeper industry exposure heightens regulatory concern. Conversely, Staff Resistance and Adoption Barriers commands the highest share of Interviewee 7's discourse, reflecting the operational focus typical of facility-management roles.

4.2.2.2 Salience of "Themes" and "Sub-themes"

Table 19 shows how widely each "Sub-theme" is shared across the seven interviewees. The top five, led by "Call for New IoT-Specific Standards and Certification" and "Limited Applicability of Current Regulations to Healthcare IoT," are mentioned by every participant, confirming that regulatory fit dominates the collective agenda. "Staff Resistance and Adoption Barriers" follows closely, recorded by six of seven respondents, underscoring the human dimension of governance challenges.

4.3 Chapter summary

This chapter has taken the reader from raw material to analytic readiness. Descriptive counts established what the interview and review corpora contain; cross-case matrices and salience showed who emphasizes which "themes" and "sub-themes"; cross-tabulation visuals revealed the relational structure that links governance, architecture, and challenge domains. With these quantitative and qualitative patterns fully mapped, the study now has a clear, transparent platform on which to build the interpretive answers to the research questions presented in the Chapter 5.

Table 18. Sub-theme Excerpt Count per Interviewee

	I1 (IT Project Manager – 5.5 years)	I2 (Co-Founder COO – 15 years)	I3 (Project/Product Manager – 9 years)	I4 (Director PM & QA – 11 years)	I5 (Director Int'l Sales)	I6 (Project Manager / Customer Success Manager – 8 years)	I7 (IT Director)
Call for New IoT-Specific Standards and Certification	2	4	8	3	6	1	1
Compliance as a 'Box-Ticking' Exercise	0	0	10	2	0	1	0
Data Privacy and Compliance Concerns (KVKK, GDPR)	0	1	7	0	0	3	1
Deficiencies in Stakeholder Knowledge and Maturity	0	0	9	1	7	4	0
Device and Network Security Risks	0	6	0	0	6	0	1
Enhancing Stakeholder Education and Training	0	0	3	2	2	3	1
Environmental and Contextual Constraints	1	2	4	0	1	1	0
Gaps in Technical and Security Regulations	1	3	6	0	1	3	0
Human and Organizational Factors (Holistic Impact)	0	0	3	1	1	1	1
Improving Project Lifecycle and Management Practices	1	5	1	2	5	2	2
Lack of Clear Standards and Certification	2	0	2	1	3	0	0
Limited Applicability of Current Regulations to IoT	2	2	8	3	4	2	2
Misalignment in Project Management and Processes	0	1	12	3	3	4	0
Prioritizing the Human Factor in Design and Processes	1	4	2	2	0	3	0
Staff Resistance and Adoption Barriers	3	5	8	3	0	1	2
Technical Implementation and Interoperability Issues	3	1	1	0	1	1	0
Use Cases and Benefits of Healthcare IoT	1	4	2	0	0	0	3

Table 19. Participant Salience of Sub-themes

Sub-theme	Interviewee Count
Improving Project Lifecycle and Management Practices	7
Limited Applicability of Current Regulations to IoT	7
Call for New IoT-Specific Standards and Certification	7
Staff Resistance and Adoption Barriers	6
Prioritizing the Human Factor in Design and Processes	5
Misalignment in Project Management and Processes	5
Human and Organizational Factors (Holistic Impact)	5
Gaps in Technical and Security Regulations	5
Environmental and Contextual Constraints	5
Enhancing Stakeholder Education and Training	5
Technical Implementation and Interoperability Issues	5
Use Cases and Benefits of Healthcare IoT	4
Data Privacy and Compliance Concerns (KVKK, GDPR)	4
Deficiencies in Stakeholder Knowledge and Maturity	4
Lack of Clear Standards and Certification	4
Compliance as a 'Box-Ticking' Exercise	3
Device and Network Security Risks	3

CHAPTER 5

FINDINGS

This chapter sets out to answer the study's three research questions by bringing together two streams of evidence: a systematic review of the literature and a series of expert interviews. The review probes why healthcare needs reference architectures for the Internet of Things and catalogues the main architectural families that scholars and standards bodies have proposed. It also surveys existing governance models to determine which challenges they address, thereby informing research question two. The interviews, meanwhile, supply first-hand accounts from clinicians, biomedical engineers, and industry practitioners, exposing the day-to-day obstacles that seldom appear in academic frameworks yet ultimately decide whether an IoT deployment succeeds or stalls.

When the two evidence streams are mapped onto the same set of thirteen challenge categories, a clear picture emerges. Academics concentrate on security, privacy, interoperability, and regulatory compliance, but pay relatively little attention to real-time performance, device lifecycle control, and most importantly human adoption issues. Practitioners confirm that security and data governance remain vital, yet insist that staff resistance, vague project goals, and a lack of workable standards routinely derail even well-engineered systems. Their testimony shows that technical safeguards alone do not guarantee operational success in a 24/7 clinical environment governed by strict data-residency rules and tight performance margins.

The chapter synthesizes these converging and diverging insights into an integrated governance model, Govern-IoT-Health, that anchors strong security and compliance controls in a broader, human-centered, and performance-aware structure.

By aligning technical design, organizational processes, and user engagement through a single governance–risk–compliance spine and a Plan–Do–Check&Act learning cycle, the model responds directly to the deficits revealed by both the literature and the interviews. In doing so, it lays the empirical and conceptual groundwork for addressing the third research question: how a new governance framework can mitigate the full spectrum of challenges confronting IoT adoption in contemporary healthcare.

5.1 Systematic literature review

This section presents the findings from the systematic literature review, structured around the study's research questions. Section 5.1.1 addresses RQ1, exploring the rationale for IoT reference architectures in healthcare and examining the types of architectures proposed. Section 5.1.2 covers RQ2, identifying existing governance frameworks and analyzing their relevance and focus within IoT-enabled healthcare contexts. Finally, Section 5.1.3 offers a synthesis of the findings, highlighting thematic patterns, gaps, and translates findings to the interview phase.

5.1.1 RQ1: Why are IoT reference architectures needed in healthcare, and what are the existing architecture types?

IoT reference architectures are vital in healthcare because they offer structured, repeatable designs to manage the integration of diverse technologies across complex and regulated environments (Nguyen et al., 2020). Without such frameworks, implementations risk becoming fragmented, insecure, and difficult to scale (Bodkhe et al., 2020). Reference architectures help standardize practices, enhance interoperability, enforce privacy and security controls, and ensure low-latency

performance through architectural elements like edge computing (Blobel, 2019; Elgammal & Krämer, 2021; Nguyen et al., 2020). By aligning technical decisions with clinical and operational needs, they support safer, more efficient, and future-ready healthcare systems.

Among 44 peer-reviewed studies (RQ1 only), five challenges recur with enough frequency to warrant explicit architectural guidance in healthcare IoT (see Figure 13): security and privacy (35 studies, 80%), interoperability (35, 80%), data management (34, 78%), scalability (25, 57%), and latency/real-time performance (22, 50 %). Each challenge spans multiple layers of an IoT stack, suggesting that a well-defined reference architecture, rather than ad-hoc system design, is the most efficient way to embed safeguards (Dang et al., 2021), provenance controls, common interfaces (Talaminos-Barroso et al., 2022), growth head-room (Akkaoui et al., 2020)., edge oriented approach to decrease latency (Kalingarani & Selvaraj, 2022).

Axial coding reorganized the open-coded reference-architecture excerpts in SLR by higher-order properties such as layer count, the presence of an edge tier, use of service orientation, security overlays, and adherence to formal standards. Constant comparison of these properties across 44 studies yielded five coherent clusters that serve as the reference-architecture types for subsequent analysis. The Three Layer Classical group, represented in 9 papers, follows the traditional perception, network, and application partition and offers minimal scalability or governance headroom (Santos et al., 2016). The Four Layer Edge Oriented cluster appears in 12 studies and introduces an edge or fog tier that preprocesses latency-sensitive data close to the patient, thereby easing cloud traffic and improving responsiveness (Firouzi et al., 2022). Another 9 papers adopt a Multi-Layer Viewpoint Service Oriented pattern that adds middleware and business or analytics views to facilitate service

orchestration and decision support in complex workflows (Pir et al., 2015).The largest group with 13 studies, is Security Focused; these designs layer blockchain, homomorphic encryption, or distributed ledger components across the stack to ensure end-to-end trust in data handling (Preetham et al., 2023). A smaller Standards Aligned category of one paper only conforms to frameworks such as ISO IEC 30141, IEEE 2413-2019, or RAMI 4.0 (Deutsches Institut für Normung, 2019; IEEE, 2020; ISO/IEC, 2024a) , thereby inheriting formal interoperability semantics and embedded governance hooks (Khan et al., 2022).

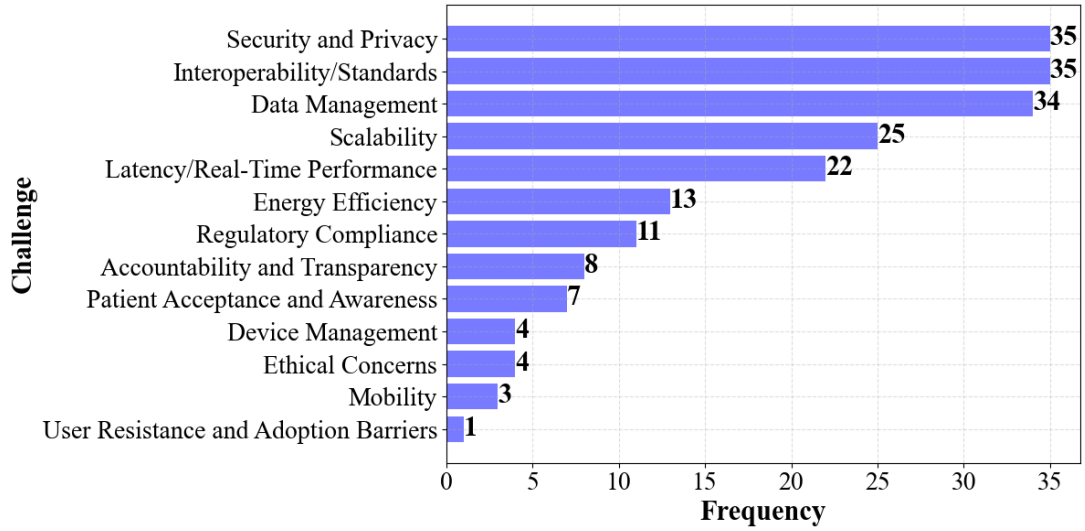

Figure 13. Frequencies of addressed challenge categories from RQ1 SLR

Figure 14 confines the heat-map to the 44 studies that address RQ1 alone, showing how healthcare reference-architecture research converges on a narrow technical core. Values calculated by each architecture types addressed challenge frequencies divided by total paper count in that category Security and privacy occupy the darkest cells in every architecture family, followed by data-management, interoperability, scalability, and real-time performance/latency confirming that these

themes receive the highest challenge coverage. By contrast, user acceptance appears only sporadically, leaving pale cells that signal minimal engagement. This pattern reflects an implicit division of labor: reference architectures operate as technical blueprints, whereas organizational and behavioral issues are expected to be tackled through governance instruments. The heat-map gaps and highlight where the forthcoming governance analysis must intervene, while confirming that the primary purpose of IoT reference architectures for healthcare is to ensure secure, interoperable, real-time performant while offering data management and scalability features for connected care.

Table 20 lists each cluster with its layer structure, characteristic attributes, representative sources and interpretation for strengths.

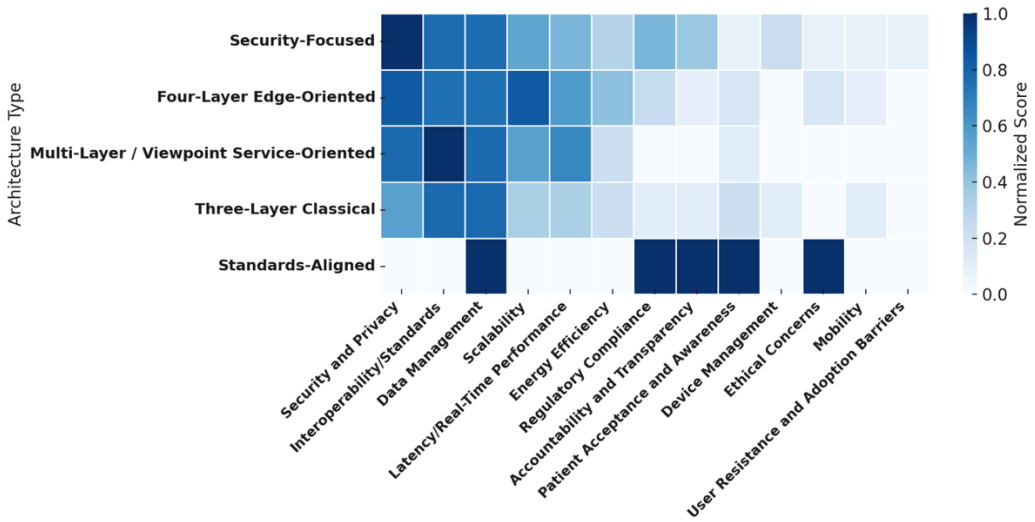

Figure 14. Reference architecture type normalized challenge coverage frequencies

Table 20. IoT Reference Architecture Types Used in Healthcare

Reference Architecture Type	Layer Structure / Views	Characteristic Attributes	Representative Papers (IDs)	Interpretation
Three-Layer Classical	Perception / Sensing – Network – Application	Minimal three-tier stack prevalent in early WBAN prototypes; limited scalability.	P11, P15, P23, P43, P49, P54, P57, P58, P71	Minimalist design for simple deployments
Four-Layer Edge-Oriented	Device – Edge / Fog – Cloud – Application	Edge/fog tier handles latency-sensitive tasks, reducing cloud traffic.	P4, P7, P25, P36, P40, P41, P45, P46, P64, P68, P69, P75	Highest in latency performance and scalability
Multi-Layer / Viewpoint Service-Oriented	Device – Network / Edge – Middleware / Platform – Application – Business / Analytics	Adds middleware and business viewpoints; supports orchestration and analytics.	P1, P9, P31, P44, P48, P52, P65, P66, P72	Middleware, business logic, and data integration
Security-Focused	Layer stack varies; security overlay (e.g., blockchain, encryption) across 3–6 layers	Introduces trust technologies (blockchain, homomorphic encryption) across layers.	P10, P14, P22, P33, P34, P42, P47, P53, P60, P61, P63, P70, P74	Strongest in privacy, trust, compliance
Standards-Aligned	Conforms to ISO/IEC 30141, IEEE 2413, RAMI 4.0, IoT-A, or similar	Inherits formal structures (IoT-A, ISO/IEC 30141, IEEE 2413) for interoperability.	P32	Aligns with ISO/IEC and IEEE frameworks

5.1.2 RQ2: Which governance frameworks are used for IoT governance, and what do they address in IoT healthcare?

This subsection critically examines how well existing IoT-healthcare governance frameworks address known challenges. Among 32 frameworks extracted from 76 SLR papers, most prioritize security and privacy (29, 91%), with significant attention also given to data management (24, 72%) and accountability and transparency (22, 66%). Interoperability (16, 50%) and regulatory compliance (19, 60%) receive moderate coverage, while categories such as latency/real-time performance (6, 19%),

device management (4, 12%), energy efficiency (2, 3%), and user resistance and adoption barriers (2, 6%) remain largely unaddressed.

Figure 15 visualizes this uneven distribution, colored cells cluster in the security column, while almost entire columns for mobility and user resistance remain blank, illustrating that most frameworks concentrate on a few tightly coupled concerns (e.g., security plus accountability) and leave other dimensions unexamined. On average, a given framework addresses just four out of 13 challenge categories.

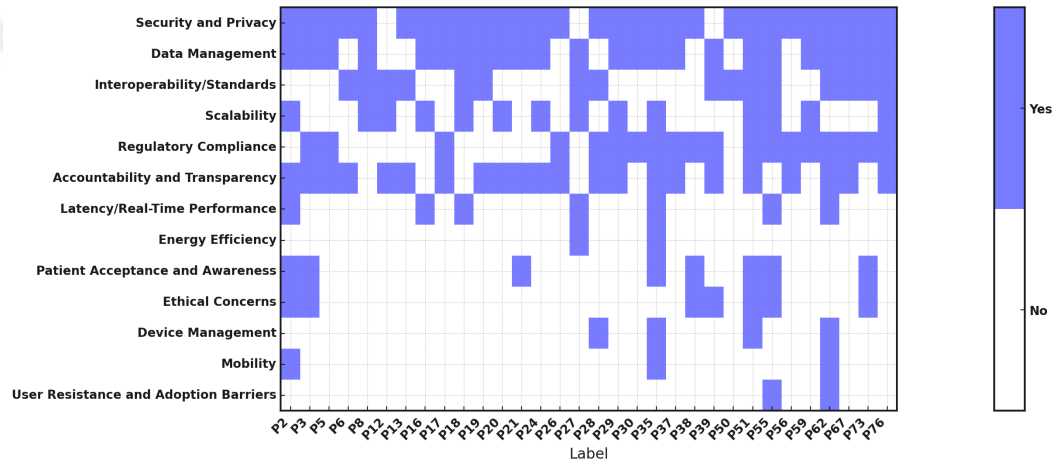

Figure 15. Framework challenge category coverage binary heat map

To highlight more comprehensive efforts, frameworks covering more than five challenge areas were shortlisted, yielding 13 studies. Filtering further by citation count (≥5 citations) narrowed the list to six (P2, P3, P35, P51, P55, P62). One, P18, was excluded due to its technical emphasis and minimal engagement with policy, stakeholder dynamics, or enforcement mechanisms. The result is a small subset of frameworks that attempt holistic governance which underscores the field's need for more integrative and multidimensional approaches.

The remaining six studies—P2, P3, P35, P51, P55, and P62—form the basis for the subsequent comparison and synthesis. Their categorical challenge coverage is detailed and compared to the proposed framework in the next section. Notably, even among the best-performing frameworks, significant gaps remain. Critical areas such as user resistance and adoption barriers are frequently overlooked or insufficiently addressed.

These empirical gaps reinforce the need to design an integrated governance framework that retains the well-supported strengths of security and compliance controls while deliberately incorporating mechanisms for real-time performance, and user resistance and adoption barriers. To inform this synthesis, the subsequent interview phase will explore how domain experts perceive these under-addressed challenges and what practical design features they believe are necessary to operationalize governance in complex, real-world healthcare IoT environments.

5.1.3 Synthesis

The systematic review provides a clear empirical baseline for the interview phase. RQ1 revealed five recurring reference-architecture types, each shaped by distinct design priorities. Security-focused and Standards-Aligned models deliver the strongest coverage for security, privacy, interoperability, and regulatory compliance, whereas Edge-Oriented and Multi-Layer designs excel at latency reduction and, to a lesser extent, scalability. Yet across all reference architecture types, there are persistent blind spots: energy efficiency, real-time performance, patient acceptance, mobility, and user resistance remain at the barely addressed for most architectures. These deficits confirm that technical blueprints alone do not guarantee operational sustainability or end-user adoption in clinical environments.

RQ2 complements this picture by assessing 32 governance frameworks. Challenge coverage frequencies (see Figure 15) show that 91% of frameworks address security and privacy, and more than two-thirds now attend to accountability and transparency. Also, this imbalance is underscored: a small cluster of frameworks repeatedly tops the strategic challenges, but no single framework spans the full spectrum.

5.2 Qualitative Interviews

5.2.1 Key healthcare IoT implementation challenges

This section addresses the primary implementation challenges in healthcare IoT, providing practitioner-driven context that informs the need for a specialized solution. While the original research question (RQ1) concerned the need for reference architectures, the interview data did not yield findings in this specific area. Therefore, this section instead focuses on a foundational research objective: Identify the principal challenges associated with implementing IoT in healthcare systems. Each interview excerpt was assigned to an SLR challenge category through careful manual reading. Each excerpt read in its full conversational context and compared its main idea with the thirteen challenge categories drawn from the systematic literature review. When an excerpt expressed more than one idea the dominant concern stated by the participant is focused. If two categories seemed plausible, the one that reflected the underlying problem was chosen rather than the surface detail. After the first round of coding, every decision is revisited to ensure that similar excerpts were treated consistently across interviews. The entire coding log was then discussed with an academic supervisor who confirmed that the category descriptions were applied in a coherent way. Although the procedure relied on a single primary coder the repeated

checking and external review provide reasonable confidence in the validity of the final category assignments.

Figure 16 shows the number of excerpts that fall into each challenge category. User resistance and Adoption Barriers appear most frequently with seventy-three excerpts. Interoperability and standards follow with thirty-one excerpts. Regulatory Compliance and Security Privacy come next with twenty-nine and twenty-seven excerpts respectively. Accountability and Transparency is least common among top five with eleven excerpts.

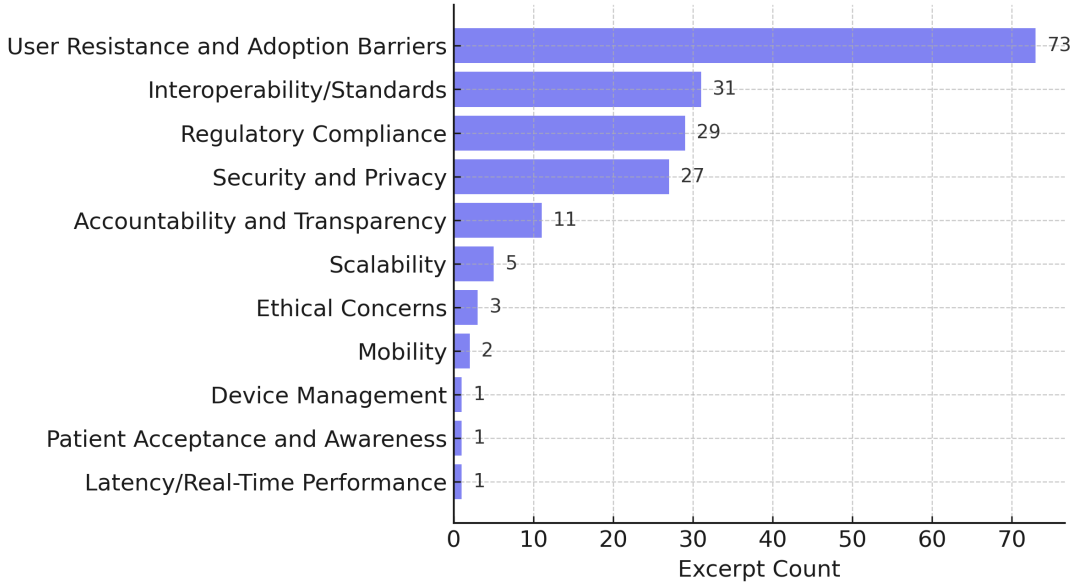

Figure 16. Frequency of coded interview excerpts per challenge category

Table 21 presents one illustrative excerpt for each of the five most prominent challenge categories, and together these quotations document how the author assigned passages to categories during coding process.

Table 21. Illustrative Excerpts for SLR Challenge Category Coding

SLR Challenge Category	Interviewee Id	Excerpt
User Resistance and Adoption Barriers	I1	". . . the team found it very difficult to persuade the public-sector personnel to use the product. Because that group lacked a sense of urgency, the team encountered serious resistance."
Interoperability/Standards	I6	"If a hospital is using an access point that does not support Bluetooth, it must recognize that Bluetooth-based real-time tracking will not be possible or very costly."
Regulatory Compliance	I3	"And on the company side, especially in Europe, it is required in some countries that this data must not leave the city or the country. In particular, there is a strong preference for keeping the data within the European Union."
Security and Privacy	I2	"A doctor's car was performing a firmware update while, at the same time, an infusion pump was transmitting data over the hospital's guest network."
Accountability and Transparency	I3	"We do not know at what point we can consider this project a success—whether it requires 100% reading accuracy or if 80% is acceptable."

In addition to the quantitative findings from the thematic analysis, qualitative insights were also synthesized by examining interview transcripts in depth. This qualitative exploration focused on the theme-area titled "Implementation Challenges in Healthcare IoT" to reveal the contextual and experiential dimensions behind the coded data.

The findings are consolidated into five key areas of challenge. A comprehensive summary of these challenges is detailed in Table 22. The most significant and pervasive challenge identified by practitioners was the human and organizational factor. This was not merely one challenge among many but was consistently described as the "biggest challenge" (I3, personnel communication, April 10, 2025) and the "outermost frame" for all other issues (I5, personnel communication, April 11, 2025). This finding is strongly supported by the high normalize1d weights of its constituent sub-themes, including "Staff Resistance and Adoption Barriers" and "Deficiencies in Stakeholder Knowledge and Maturity" Interviewees described a multi-layered problem, including active resistance from public-sector staff with low accountability (I1, personnel communication, April 9, 2025), and passive resistance from overworked clinicians who de-prioritize any task

not directly related to patient care (I2, personnel communication, April 10, 2025). This resistance is fueled by a lack of technical maturity across all levels, from end-users to procurement managers, who may request technology based on "buzzwords" rather than a clear purpose (I3, personnel communication, April 10, 2025) or struggle to grasp the system's benefits (I5, personnel communication, April 11, 2025). The consequences are severe, leading to projects where expensive systems are installed but remain "unused due to a lack of user support" (I4, personnel communication, April 11, 2025).

The second major challenge lies in widespread misalignment and immaturity in project management and processes. The sub-theme "Misalignment in Project Management and Processes" was one of the most heavily weighted in the study, indicating its critical importance. Practitioners described a frequent and damaging disconnect between the project's buyers and its end-users (I4, personnel communication, April 11, 2025), leading to solutions that are not fit for purpose. A critical failure point is the beginning of the project lifecycle, where vague or unrealistic specifications create a cascading effect of problems (I3, personnel communication, April 10, 2025). As one interviewee lamented, "We don't know at what point we can call this project successful . . . we don't know this" (I3, personnel communication, April 10, 2025). This lack of clear goals and success metrics leads to wasted resources, project delays, and systems that are ultimately built "for show" rather than for function (I3, personnel communication, April 10, 2025). Third, the analysis revealed a foundational challenge stemming from a lack of clear technical standards and resulting interoperability issues.

Table 22. Interview Key Findings for Healthcare IoT Implementation Challenges

Description	Supporting Sub-themes	Interviewee Ids	Sample Excerpts
The primary obstacle to successful implementation is human and organizational. It includes active and passive resistance from staff (due to workload, culture, or fear), coupled with a profound lack of technical knowledge and maturity among all stakeholders, from end-users to buyers.	Staff Resistance and Adoption Barriers Deficiencies in Stakeholder Knowledge and Maturity	I1, I2, I3, I4, I5, I6, I7	I1: "Persuading public personnel to use the product was the most problematic part for us." I3: "The lack of knowledge about what is wanted in the specification, plus the users of the given solution not understanding why they are using it, is one of the biggest problems."
Projects are frequently undermined by flawed processes, including a disconnect between procurement and implementation teams, a failure to define clear success metrics, and unrealistic requirements. These initial errors create cascading negative effects throughout the project lifecycle.	Misalignment in Project Management and Processes	I2, I3, I4, I6	I3: "We don't know at what point we can call this project successful, with 100% reading guarantee or 80% success, we don't know." I4: "The people who buy the product and the people who implement the product can be different."
The absence of clear, global, or even national standards for healthcare IoT creates significant uncertainty and technical risk. This lack of standardization complicates technology and vendor selection and turns every system integration into a bespoke, high-risk experiment.	Lack of Clear Standards and Certification Technical Implementation and Interoperability Issues	I1, I3, I4, I5, I6	I1: "There was no complete standard for this in the world . . . We didn't know which RFID technology to choose and how to use it." I5: "The issue of when and at what step integration can be done in these interoperability processes turns into an experimental area in every project."
The physical and operational environment of hospitals poses unique challenges. These include the immense scale of facilities, which creates scalability and device management issues; the 24/7 operational tempo, which complicates deployment; and physical interference from building materials that can degrade technology performance.	Environmental and Contextual Constraints Technical Implementation and Interoperability Issues (related to scale)	I1, I2, I3, I6	I2: "You don't have such a luxury in Brownfield hospitals. That hospital works 24/7, and you have to do these installations within this working hospital." I1: "The large scale of the project . . . was a direct cause of technical difficulties."
High-Stakes Nature of Use Cases Amplifies All Other Challenges The critical nature of healthcare IoT applications, from preventing infant abduction to ensuring patient safety, means that there is zero tolerance for error. This high-stakes context dramatically amplifies the importance of all other challenges, making user trust, system reliability, and robust processes non-negotiable requirements.			

While not the most heavily emphasized topic, the absence of a "global IoT standard" (I1, personnel communication, April 9, 2025) was identified as a root cause of significant uncertainty and risk.

Third, the analysis revealed a foundational challenge stemming from a lack of clear technical standards and resulting interoperability issues. While not the most heavily emphasized topic, the absence of a "global IoT standard" (I1, personnel communication, April 9, 2025) was identified as a root cause of significant uncertainty and risk. This forces vendors and hospitals into a state where every integration becomes a new "experiment" (I5, personnel communication, April 9, 2025), increasing the risk of failure. This was highlighted with concrete examples of project setbacks, such as purchasing access cards that were incompatible with the specified readers, a failure that could have been avoided with clear, upfront standards (I1, personnel communication, April 9, 2025).

Fourth, the unique environmental and contextual constraints of hospitals create significant technical and operational hurdles. The sheer physical and operational scale of modern hospitals was a recurring challenge. The vastness of facilities contributes to asset loss and necessitates complex, large-scale labeling and tracking initiatives, a major scalability problem (I1, personnel communication, April 9, 2025). Furthermore, the 24/7, non-stop nature of "brownfield" hospitals means that system deployments must be conducted in a live environment without any downtime, a logistical constraint rarely faced in other industries (I2, personnel communication, April 10, 2025). Participants also noted how specific environmental factors, such as the presence of large metal structures, can directly interfere with the performance of RF-based technologies like UHF RFID (I3, personnel communication, April 10, 2025).

Finally, the analysis shows that the high-stakes nature of healthcare IoT use cases amplifies the severity of all other challenges. The applications discussed were not trivial; they included ensuring baby safety, preventing psychiatric patient elopement, and confirming the calibration of life-critical medical devices (I2, I3, personnel communication, April 10, 2025). A system failure in this context is not an inconvenience but a potentially fatal event. This reality explains why user trust is so fragile, "a third chance is generally not given" (I2, personnel communication, April 10, 2025), and why the reliability and security of these systems are paramount. The immense potential of these use cases is matched only by the immense risk of their failure, making the resolution of all other implementation challenges an absolute necessity.

5.2.2 RQ2. Which governance frameworks are used for IoT governance, and what do they address in IoT healthcare?

The findings presented here were synthesized from the thematic analysis of the interview transcripts, focusing on excerpts which are under the "Governance, Risk, and Compliance (GRC) Landscape" theme-area. Individual codes and sub-themes were aggregated into seven distinct key findings that represent recurring patterns and significant insights shared across the interviews. A full summary of these findings is presented in Table 23.

The analysis reveals that the current application of governance frameworks in healthcare IoT is both limited and widely perceived as inadequate. ISO 27001 was identified as the most prevalent framework, often adopted to meet contractual or financing requirements (I1, personnel communication, April 9, 2025; I4, personnel communication, April 11, 2025; I7, personnel communication, April 12, 2025;).

However, the broader portfolio of established governance tools appears largely unused in practice. Notably, other key frameworks like COBIT demonstrated exceptionally low awareness among practitioners, with one experienced professional stating they had "never heard of it" before the interview (I2, personnel communication, April 10, 2025). This suggests that the practical governance toolkit being applied in the field is significantly narrower than what is available in theory.

More importantly, the frameworks that are in use are considered insufficient for the specific challenges of healthcare IoT. This perception is a dominant finding, the sub-theme "Limited Applicability of Current Regulations to IoT", the second most emphasized concept in the entire study. Participants consistently argued that standards like ISO 27001 are too generic and process-oriented, fundamentally failing to address the tangible, hardware-centric risks of what they termed "device security" (I2, personnel communication, April 11, 2025; I5, personnel communication, April 11, 2025). This leaves a critical gap in the governance of physical IoT components and their unique vulnerabilities. As one interviewee summarized, "I don't think the current standards are sufficient for managing IoT risks; these standards were not ready for IoT" (I1, personnel communication, April 9, 2025). Beyond the limitations of the frameworks themselves, the research uncovered significant challenges in how governance is practiced organizationally. A recurring finding was the prevalence of a superficial, "box-ticking" approach to compliance (I3, personnel communication, April 10, 2025; I4, personnel communication, April 11, 2025; I6, personnel communication, April 11, 2025;). In this model, the primary objective shifts from genuine risk mitigation to the mere acquisition of certificates (e.g., CE, JCI) to satisfy external stakeholders or regulatory mandates.

Table 23. Interview Key Findings on The GRC Landscape in Healthcare IoT

Key Finding Description	Related SLR Challenge Category	Related Sub-themes	Interviewee Ids	Sample Excerpts
ISO 27001 is the most prevalent IT governance framework in use, but its application is often limited to general information security. Other frameworks like COBIT have very low awareness and adoption among practitioners.	Interoperability/Standards, Regulatory Compliance, Patient Acceptance and Awareness	Limited Applicability of Current Regulations to IoT Compliance as a 'Box-Ticking' Exercise	I1, I2, I4, I5, I6, I7	I2: "I see it as a personal shortcoming that I had never heard of COBIT; I actually learned about it through this interview." I7: "In our solutions, ISO 27001 is already our fundamental guideline."
Existing governance models like ISO 27001 are widely considered insufficient for managing the unique risks of healthcare IoT. They are perceived as being too general, overly focused on process, and failing to address hardware-specific challenges like ""device security"".	Security and Privacy, Interoperability/Standards	Limited Applicability of Current Regulations to IoT, Gaps in Technical and Security Regulations	I1, I2, I3, I5, I6	I2: "In my opinion, ISO 27001 focuses more on procedural information security; in the context of IoT, especially on the device security side, it may leave gaps." I5: "I do not believe that ISO 27001 standards can be fully applied to IoT products in every sense."
The application of governance is often reduced to a superficial 'box-ticking' exercise. The primary goal becomes acquiring certifications (e.g., CE, JCI) to meet external demands, rather than a deep, internalized commitment to improving security and quality.	Regulatory Compliance, Accountability and Transparency, User Resistance and Adoption Barriers	Compliance as a 'Box-Ticking' Exercise	I3, I4, I6	I3: "Actually, it seems that hospitals are doing this not because they are fully aware and willing, but with a mindset of ‘we need to do it, so let’s do it’." I4: "Sometimes these systems are purchased just to fulfill regulatory requirements."
Data privacy regulations (e.g., GDPR) are a primary driver of security governance but also introduce significant implementation challenges. Strict data residency rules conflict with global business models, and pervasive privacy fears can act as a barrier to essential system integrations.	Security and Privacy, Regulatory Compliance, Ethical Concerns	Data Privacy and Compliance Concerns (KVKK, GDPR), Device and Network Security Risks	I2, I3, I5, I6, I7	I2: "Even basic integrations are not being carried out due to data security concerns . . . Even Active Directory integration is postponed by saying ‘let’s not activate it for now’." I3: "This contradiction [data residency vs. global teams] reveals the need for new governance mechanisms both legally and administratively."
Governance frameworks and their principles are often siloed within IT departments. They are not effectively disseminated to or adopted by other clinical and operational departments, which prevents an enterprise-wide culture of governance and creates accountability gaps.	Accountability and Transparency, User Resistance and Adoption Barriers	Limited Applicability of Current Regulations to IoT	I5	I5: "Governance issues have remained within the IT departments of hospitals. It is not a topic that has spread across the entire hospital."
Regulatory and certification frameworks have not kept pace with IoT innovation, leading to significant compliance challenges. Novel, hybrid IoT products often lack clear categories, creating ambiguity in testing requirements and certification pathways.	Regulatory Compliance, Interoperability/Standards, Security and Privacy, Ethical Concerns	Gaps in Technical and Security Regulations, Limited Applicability of Current Regulations to IoT	I3, I5	I3: "We struggle to find a category to define the product while applying for CE certification. Because we cannot determine the exact category, we apply under what we think is the closest—sometimes even two categories to avoid risk."
The lack of comprehensive, official IoT standards creates significant security risks and inefficiencies. Specific gaps include the absence of clear guidelines on device security, network segmentation policies, and operational procedures, forcing vendors and hospitals to operate in a high-risk, ad-hoc manner.	Security and Privacy, Interoperability/Standards, Device Management	Device and Network Security Risks, Gaps in Technical and Security Regulations, Lack of Clear Standards and Certification	I2, I4, I5	I2: "While a doctor’s Tesla is updating its firmware, an infusion pump in the hospital is simultaneously transmitting data over the guest network." I5: "With on-prem projects, you are also required to purchase serious cybersecurity tools. They are not doing this."

One participant described this attitude as, "it's not that the hospitals are doing this consciously, but more with an 'it has to be done, so let's do it' approach" (I3, personnel communication, April 10, 2025). This behavior was strongly linked by interviewees to "Deficiencies in Stakeholder Knowledge and Maturity", suggesting that when organizational maturity is low, compliance becomes a performative act rather than an internalized value.

This issue is compounded by the organizational siloing of governance. As one participant emphatically noted, "Governance topics are an issue that remains within the IT departments in the hospital. It is not a subject that has spread to the hospitals in general" (I5, personnel communication, April 11, 2025). This failure to disseminate governance principles to clinical and operational units, who are critical stakeholders in any IoT system, prevents the development of an enterprise-wide culture of accountability and creates dangerous disconnects between policy and practice.

The combination of inadequate frameworks and flawed practices results in significant unaddressed risks and regulatory friction. While data privacy regulations like GDPR are actively enforced, they present a double-edged sword. Interviewees noted that strict data residency rules and pervasive privacy fears create significant barriers to system integration and global collaboration, sometimes hindering the very data analysis the IoT systems are meant to enable (I2, personnel communication, April 10, 2025; I3, personnel communication, April 10, 2025). Furthermore, the regulatory landscape has failed to keep pace with technological innovation. Participants described major challenges in achieving compliance for novel, hybrid IoT products, as existing certification pathways lack appropriate categories, forcing vendors into costly and inefficient workarounds (I3, personnel communication, April

10, 2025). This regulatory vacuum contributes directly to tangible security risks, such as connecting critical medical devices to insecure guest networks (I2, personnel communication, April 10, 2025) or forgoing essential cybersecurity investments for on-premises solutions (I5, personnel communication, April 11, 2025).

In summary, the governance landscape for healthcare IoT as described by the study participants is characterized by a reliance on a narrow set of ill-fitting, general-purpose frameworks. Their application is often superficial, organizationally siloed, and unable to address the specific device-level and regulatory challenges posed by modern IoT technology. This creates a significant gap between the theoretical promise of governance and its practical, and often flawed, implementation in the field.

5.2.3 RQ3. Insights

The insights are synthesized from the thematic analysis, primarily drawing from the "Pathways to an Improved Governance Framework" theme-area. These findings represent a practitioner-driven vision for a more effective governance model. A summary of these findings is provided in Table 24.

The analysis reveals that a new, effective governance framework cannot be a monolithic document but must be a multi-faceted system built on four interconnected principles: (1) the establishment of fit-for-purpose standards, (2) the prioritization of the human factor, (3) the adoption of adaptive project management practices, and (4) the implementation of robust enforcement mechanisms.

The foundational and most heavily emphasized dimension is the establishment of fit-for-purpose standards and certifications. This was the most significant proposal from the interviewees, underscored by "Call for New IoT-Specific Standards and

Certification". Participants argued that the current ad-hoc environment, where every hospital creates its own specifications (I4, personnel communication, April 11, 2025), is a root cause of inefficiency and risk. The proposed solution is a new set of clear, authoritative standards developed through a multi-stakeholder process involving regulators, technology experts, medical device manufacturers, and end-users (I5, personnel communication, April 11, 2025). These standards must address specific IoT challenges, such as cybersecurity, device interoperability (e.g., mandating HL7 integration (I5, personnel communication, April 11, 2025)), frequency compatibility (I5, personnel communication, April 11, 2025), and even standardized operational procedures, like where to place a patient's wristband in different clinical scenarios (I5, personnel communication, April 11, 2025). As one participant stated, "if a new governance scope or mechanism for IoT and health is established, such decisions can be made more consciously" (I3, personnel communication, April 10, 2025).

The second dimension of the proposed framework is a deep and sustained prioritization of the human factor, driven by education and human-centered design. While standards provide a technical foundation, interviewees recognized that they are ineffective without user acceptance. This finding directly addresses the challenges of "Staff Resistance and Adoption Barriers" and "Deficiencies in Stakeholder Knowledge and Maturity". The proposed solutions call for a cultural shift away from a technology-centric view. This includes implementing continuous education and training programs to enhance stakeholder awareness at all levels, from clinicians to procurement managers (I3, personnel communication, April 10, 2025; I5, personnel communication, April 11, 2025; I6, personnel communication, April 11, 2025).

Table 24. Interview Key Findings for Development of a New Healthcare IoT Governance Framework

Description	Supporting Sub-themes	Interviewee Ids	Sample Excerpts
The framework must be built on a foundation of clear, IoT-specific standards covering security, interoperability (e.g., HL7), frequency compatibility, and operational procedures. These standards should be developed collaboratively by regulators, vendors, and users to ensure relevance and buy-in.	Call for New IoT-Specific Standards and Certification Improving Project Lifecycle and Management Practices	I1, I2, I3, I4, I5, I7	I3: "Here, if a new governance scope or mechanism specific to IoT and health were put forward, decisions like these could be made more consciously." I5: "The standards for interaction in the frequency dimension of products with other products and hardware within the hospital need to be clear."
The framework must mandate a human-centric approach to counter user resistance and low maturity. This involves continuous, role-based education to build awareness and a commitment to user-centered design principles, ensuring solutions are intuitive and solve real-world problems.	Prioritizing the Human Factor in Design and Processes Enhancing Stakeholder Education and Training	I1, I2, I3, I4, I5, I6	I2: "Technology companies should be in love with the problem they are trying to solve, not their products." I6: "Designing while listening to the person who uses the product and lives the process is, I think, important."
The governance model should promote flexible, iterative, and adaptive project management. This moves away from rigid, static plans and embraces concepts like treating initial workflows as testable "hypotheses," transparent risk management, and the ability to evolve solutions based on real-world feedback.	Improving Project Lifecycle and Management Practices	I1, I2, I4, I5, I6, I7	I2: " . . .a customizable, evolvable workflow management structure, where we call the initial workflow a hypothesis . . . is very critical." I2: "Knowing how to move forward with new ways, as much as being able to abandon the product when necessary, should be the greatest competence of a technology provider."
To ensure compliance is meaningful and not just a "box-ticking" exercise, the framework must include mechanisms for strong enforcement. This involves independent, spontaneous audits with real consequences for non-compliance, up to and including the suspension of operations.	Call for New IoT-Specific Standards and Certification	I2	I2: " . . .instead of going from planned and known scenarios, I think there should be more spontaneous controls here." I2: "I believe that independent security units should audit hospitals, and if certain criteria are not met, the hospital's activities should be temporarily suspended."

Furthermore, it demands a commitment to human-centered design, where end-users are involved in the design process (I6, personnel communication, April 11, 2025), and vendors are encouraged to be "in love with the problem they are trying to solve, not their products" (I2, personnel communication, April 10, 2025), ensuring that solutions are intuitive and genuinely address user needs.

Third, participants advocated for adopting agile and adaptive project and lifecycle management practices. This proposal addresses the perceived failure of rigid, top-down implementation models. The sub-theme "Improving Project Lifecycle and Management Practices" mentioned frequently, indicating a strong desire for more dynamic processes. The vision is for a framework that supports iterative development, where initial workflows are treated as "hypotheses" to be tested and evolved (I2, personnel communication, April 10, 2025). This includes demands for transparent risk management from the project outset (I2, personnel communication, April 10, 2025) and an embrace of iteration, where vendors have the competency to adapt or even "abandon a product" if it fails to meet user needs (I2, personnel communication, April 10, 2025). This adaptive approach is seen as critical for navigating the complex and ever-changing hospital environment.

Finally, to counteract the "box-ticking" culture identified in the GRC analysis, the proposed framework includes robust, independent auditing and enforcement mechanisms. Participants argued that standards without consequences are meaningless. They proposed a new system of accountability with real authority, including "spontaneous controls" rather than predictable annual checks (I2, personnel communication, April 10, 2025). Most powerfully, it was suggested that independent bodies should have the power to enforce compliance with severe penalties, up to and including the temporary "suspension of a hospital's operations" for non-compliance

(I2, personnel communication, April 10, 2025). This call for authoritative enforcement is seen as essential for ensuring that governance principles are taken seriously and are translated into meaningful action.

In conclusion, the practitioners envision a holistic governance framework that is purpose-built, human-centric, agile, and authoritative. It moves beyond the limitations of existing models by creating clear and relevant standards, fostering a culture of acceptance through education, managing projects with flexibility, and ensuring accountability through meaningful enforcement.

5.2.4 Synthesis

The preceding sections have detailed the findings from the interviews, systematically exploring the principal challenges of healthcare IoT implementation (RQ1-focused analysis), the inadequacies of the current governance landscape (RQ2), and the practitioner-driven requirements for an improved framework (RQ3). This section synthesizes these disparate findings into a cohesive narrative, demonstrating how the proposed solutions directly address the identified problems.

The analysis of implementation challenges revealed a complex, interconnected web of issues, quantitatively dominated by human and organizational factors. User resistance and adoption barriers category emerged as the most prominent challenge category, in frequency. This was not a simple matter of opposition to new technologies but was rooted in deeper issues of low stakeholder maturity, the intense workload of clinicians, and a cultural disconnect where operational IoT systems are de-prioritized in favor of direct clinical technologies. This core human challenge was exacerbated by widespread misalignment in project management, where a lack of clear goals, poor communication between buyers and

users, and vague specifications led to failed or under-utilized projects. These human-centric problems were compounded by technical hurdles, including a lack of clear interoperability standards, significant security and compliance risks, and the unique contextual constraints of the 24/7 hospital environment.

When examining the current governance landscape, it became clear that existing frameworks are failing to mitigate these challenges. The analysis showed a heavy reliance on a single, general-purpose standard, ISO 27001, which practitioners deemed insufficient for the hardware-specific risks of IoT. The application of this and other regulations was often described as a superficial, "box-ticking" exercise, driven by external mandates rather than an internalized commitment to quality. This culture, fueled by low stakeholder maturity, means that even when a framework is officially "in use," it often fails to influence practice meaningfully. The result is a governance vacuum where critical risks, from device-level vulnerabilities to insecure network configurations, are left unaddressed. The proposed solutions for a new governance framework, derived from RQ3, can be understood as a direct response to these identified failures. The practitioners' vision is not for another static document but for a holistic, multi-faceted system designed to counteract the specific problems they face. The foundational proposal, the establishment of fit-for-purpose standards, directly addresses the chaos of ad-hoc specifications and interoperability failures. The call to prioritize the human factor through education and human-centered design is a direct remedy for the dominant challenge of user resistance and low maturity. The advocacy for agile and adaptive project management targets the failures of rigid, misaligned project planning. Finally, the demand for robust, independent enforcement is a clear countermeasure to the ineffective "box-ticking" culture.

In essence, the research journey from challenges to solutions reveals a clear causal chain: ill-fitting and poorly implemented governance causes implementation challenges, particularly those related to human factors and process maturity. In turn, the practitioners' vision for an ideal framework is one that systematically dismantles these challenges by being purpose-built, human-centric, agile, and authoritative. The relationship between the most prominent challenges and the proposed pillars of a new governance framework is summarized in Table 25. This table serves as a bridge, mapping the problems identified by practitioners to the solutions they envision, providing a coherent and empirically grounded model for improving healthcare IoT governance. This synthesis directly informs the final proposed framework.

Table 25. Synthesis of Interview Findings

Dominant Challenge Area (From RQ1 & RQ2 Analysis)	Illustrative Practitioner Quote on the Challenge	Corresponding Pillar of the Proposed Governance Framework (From RQ3 Analysis)	Illustrative Practitioner Quote on the Solution
Human & Organizational Factors (User Resistance, Low Maturity, Misaligned Goals)	"The human factor is the biggest challenge. It affects project management, technical implementation, and sustainability." (I3, personnel communication, April 10, 2025)	Prioritize the Human Factor through Education & Human-Centered Design	"The fundamental issue that needs to be addressed is the human one. These people should be considered together with the products and processes they use, and each should be iterative." (I2, personnel communication, April 10, 2025)
Inadequate Standards & Interoperability Failures (Vague Specifications, Integration "Experiments", Technical Incompatibility)	"Because there is no standard for this in the world, we didn't know which RFID technology to choose or how to use it." (I1, personnel communication, April 9, 2025)	Establish Fit-for-Purpose, Multi-Stakeholder Standards & Certifications	"If a new governance scope or mechanism specific to IoT and health were put forward, decisions could be made more consciously." (I3, personnel communication, April 10, 2025)
Flawed Project Management & Process Misalignment (Disconnect between Buyers/Users, Lack of Success Metrics, Rigid Planning)	"We do not know at what point we can consider this project a success, whether it requires 100% reading accuracy or if 80% is acceptable." (I3, personnel communication, April 10, 2025)	Adopt Agile and Adaptive Project Lifecycle & Management Practices	" . . .a customizable, evolvable workflow management structure, where we call the initial workflow a hypothesis . . . is very critical." (I2, personnel communication, April 10, 2025)
Ineffective Compliance & Security Gaps ("Box-Ticking" Culture, Siloed Governance, Unaddressed Risks)	"It's not that hospitals do this consciously, but more with an 'it has to be done, so let's do it' approach." (I3, personnel communication, April 10, 2025)	Implement Robust, Independent Auditing and Enforcement Mechanisms	"I believe that independent security units should audit hospitals, and if certain criteria are not met, the hospital's activities should be temporarily suspended." (I2, personnel communication, April 10, 2025)

5.3 Integrating findings

Since interview findings does not have a RQ1 finding IoT challenge coverage will be compared. To draw the separate strands of evidence together, the study now compares the reliability-weighted findings from the systematic review with the supporting evidence from interviews along with evidence strength. This integrated view reveals where academic models and practitioner experience converge and where they diverge, thereby identifying the challenges that must be covered in the design of a new governance framework.

Table 26 aligns the literature tiers with frontline testimony and clarifies how each challenge unfolds in practice. Security & privacy retains a very-high priority, yet practitioners widen its scope: vulnerabilities now include low-voltage and building-management networks, prompting a niche cybersecurity market (I5, personal communication, April 11, 2025; I6, personal communication, April 11, 2025; I2, personal communication, April 10, 2025). Data-management issues remain acute, but the emphasis shifts from storage volume to rapid fault-finding and multi-source analytics (I1, personal communication, April 9, 2025; I2, personal communication, April 10, 2025). Interoperability is still rated very high; teams struggle to decide where in the data flow to integrate, and legacy Wi-Fi without Bluetooth blocks entire use cases (I5, personal communication, April 11, 2025; I6, personal communication, April 11, 2025). The review's high-tier items also resonate. Scalability proves partly social: two-million-item inventories and device hoarding create untracked complexity that technical scaling alone cannot fix (I1, personal communication, April 9, 2025). Latency / real-time performance is tied directly to patient safety, sub-second indoor-navigation alerts drive rapid clinical response, so latency KPIs belong on governance dashboards (I7, personal communication, April

12, 2025; I2, personal communication, April 10, 2025). Lower-tier themes draw less attention. Energy efficiency surfaces only when lower-power tags also reduce cost (I5, personal communication, April 11, 2025). Regulatory compliance is acknowledged but fragmented; EU data-locality rules differ from national mandates, implying modular, jurisdiction-aware controls (I3, personal communication, April 10, 2025).

These converging lines of evidence strengthen confidence that the reference architectures cited in this study respond to the field's most urgent demands. At the same time, they underline the need for complementary governance instruments that translate architectural capabilities into usable, compliant, and scalable clinical solutions.

User resistance and adoption barriers category dominate the findings in Table 27 and emerge as a silent but decisive threat to project success. Interviewees repeatedly pointed to persistent resistance among end-users, both staff and, to a lesser extent, patients who are expected to operate IoT tools. Public-sector personnel were reported to "lack concern" and actively avoid new systems; emergency events (e.g., a "code pink") were sometimes required before reluctant users adopted the technology. Narratives of alarm fatigue, misconceptions such as "staff are being tracked with chips" and uncertainty about success criteria (80% vs 100% read accuracy) show how unclear value propositions erode trust. Even technical fixes, simplified interfaces, workflow customization, or consent forms under data-protection law, did not fully eliminate these behavioral hurdles. Participants therefore framed the "human factor" not as a peripheral issue but as the primary determinant of adoption, emphasizing that users must perceive direct benefit and minimal disruption before they will engage with IoT workflows.

Table 26. SLR Most Covered IoT Challenges and Related Interview Evidence

IoT Challenge Category	SLR Tier	Supporting Evidence from Interviews	Interpretation
Security and Privacy	Very High	"Especially because they have seen that security issues related to medical devices have reached very serious levels, start-ups specialized in healthcare cybersecurity have started to emerge in the market."(I5, personnel communication, April 11, 2025) "At this point, a security vulnerability may occur; for example, problems can arise while transferring the patient's data or during masking."(I6, personnel communication, April 11, 2025) "Especially in certain networks such as building management systems or areas involving low-voltage systems, the security perspective tends to be somewhat overlooked."(I6, personnel communication, April 12, 2025) "The security of devices has become a critical concern."(I2, personnel communication, April 10, 2025)	Practitioners reinforce the SLR ranking but add nuance: threats no longer center only on patient data; 'peripheral' systems (BMS, low-voltage) now enlarge the attack surface, prompting a dedicated start-up ecosystem. This suggests existing frameworks underplay vertically-integrated security and market dynamics.
Data Management	Very High	"In the first hospital, we initially faced significant challenges due to the large data volume and the scale of the infrastructure; it was difficult to identify the issues because of the high number of RFID readers."(I1, personnel communication, April 9, 2025) "The true strength of IoT systems lies in their ability to generate new and more effective insights by correlating data from multiple sources." (I2, personnel communication, April 10, 2025)	Interviews confirm volume/variety issues but shift the emphasis from storage to diagnostic agility and analytic insight, indicating that governance should prioritize quality-assured data pipelines over raw capacity.
Interoperability -Standards	Very High	"For instance, in the healthcare domain, there is the issue of interoperability. The main concern here is determining when and at which stage integration should take place within these interoperability processes — and in every project, this turns into a kind of experimentation field all over again."(I5, personnel communication, April 11, 2025) "If a hospital is using an access point that does not support Bluetooth, it needs to be aware that real-time tracking based on Bluetooth will not be possible or feasible."(I6, personnel communication, April 11, 2025)	Interviews uphold the SLR's "very high" rating for interoperability yet expose two gaps: teams struggle to decide where in the data flow to integrate, leading to costly trial-and-error, and legacy hardware such as non-Bluetooth access points can still block standards-compliant solutions. Governance may therefore pair protocol alignment with clear integration-timing rules and forward-looking procurement.
Scalability	High	"There were approximately 2 million inventory items in the hospital, and these needed to be tagged, accurately named, and properly located, which was quite challenging."(I1, personnel communication, April 9, 2025) "Due to the large size of the hospital, inventory items were frequently lost; sometimes, staff would hide devices thinking they might be needed later."(I1, personnel communication, April 9, 2025)	Beyond system load, scalability is social: human work-arounds (device hoarding) generate untracked complexity. Frameworks therefore need socio-technical controls (awareness, incentives) alongside technical capacity planning.
Latency/Real-Time Performance	High	"Therefore, for operational purposes such as responding rapidly to incoming calls or managing internal logistics, we utilize location-based indoor navigation systems integrated with RFID, wireless connectivity, and beacons to enable real-time positioning. This infrastructure supports low-latency decision-making in time-critical scenarios."(I7, personnel communication, April 12, 2025) "Staff members can request assistance from anywhere within the hospital by sending an alert along with their real-time location information, enabling a rapid response."(I2, personnel communication, April 10, 2025)	Practitioners confirm latency as an operational imperative and link it directly to patient safety and logistics efficiency, suggesting latency KPIs should be elevated in governance dashboards rather than treated as a purely technical QoS metric.
Energy Efficiency	Average	"If I can solve this not with UHF passive RFID, but with Angle-of-Arrival tags that can say 'I'm here' four times a second and operate at a lower power level and cost…"(I5, personnel communication, April 11, 2025)	The quote shows energy efficiency is a secondary concern, considered when convenient, not as a core priority.
Regulatory Compliance	Average	"And on the company side, especially in Europe, there are cases where data is not allowed to leave certain countries or even specific regions; in particular, when it comes to the European Union, there is a strong requirement that data must not be transferred outside the EU."(I3, personnel communication, April 10, 2025) "In some countries, the regulatory requirements come from the ministry of health, while in others, they are issued by state-level healthcare authorities."(I3, personnel communication, April 10, 2025)	Evidence corroborates SLR concerns but highlights diverging jurisdictional layers, implying governance mechanisms must be modular enough to address both national and supra-national mandates.

Taken together, the evidence suggests that technical excellence alone is insufficient. Security, data, and standards problems will persist, yet they can usually be mitigated with engineering effort and regulatory compliance. By contrast, user resistance and adoption barriers appear across almost every project stage from procurement and installation to everyday operation and can negate otherwise robust solutions. A governance framework for IoT in healthcare must therefore embed structured change-management processes, continuous training, and transparent communication to convert skeptical stakeholders into active participants. Without addressing these social-behavioral constraints, even the most secure, interoperable, and scalable IoT systems risk limited uptake and diminished clinical impact.

Although a handful of studies supply robust controls for security, compliance, and transparency, the interviews reveal that these same areas remain pain points in daily practice. Practitioners report that such mechanisms rarely penetrate routine workflows, are applied mainly as certificate-seeking exercises, and leave device-level risks, performance tight spots, and human-factor barriers largely untouched. Next, interview data is used to explain why these gaps persist and how organizations improvise around them.

Interview testimony shows that the governance toolkit in everyday practice is narrow and often ill-suited to connected-device risks. One engineer admitted, “I see it as a personal shortcoming that I had never heard of COBIT; I actually learned about it through this interview” (I2, personal communication, April 10, 2025). Even the standard most widely used, ISO/IEC 27001, is applied largely for contractual reasons rather than fitness for purpose, as one vendor stated, “In our solutions, ISO 27001 is already our fundamental guideline” (I7, personal communication, April 12, 2025).

Table 27. SLR Least Covered IoT Challenges and Related Interview Evidence

IoT Challenge Category	SLR Tier	Supporting Evidence from Interviews	Strength of Evidence
Accountability and Transparency	Average	"So, at what point can we consider this project a success — is it with a 100% read accuracy guarantee, or 80% success? We simply don't know."(I3, personnel communication, April 10, 2025) "Governance matters have largely remained within the IT departments of hospitals and have not been adopted across the broader hospital structure."(I5, personnel communication, April 11, 2025) "At the project approval stage, it was often quite difficult to get individuals to accept the provisions that had been specifically developed and included in the contract."(I6, personnel communication, April 11, 2025)	High
Patient Acceptance and Awareness	Average	"Since we were tracking our patients under the scope of KVKK (Turkish Personal Data Protection Law), we had to obtain a consent form from them… Patients generally did not resist much in this regard, as we were ensuring their safety—especially concerning baby abduction cases."(I1, personnel communication, April 9, 2025)	Low
Device Management	Average	"We began tracking the maintenance and calibration processes of devices using RFID technology; any errors in the calibration of medical devices could lead to serious problems for patients." (I1, personnel communication, April 9, 2025)	Low
Ethical Concerns	Average	"In the beginning, for instance, one of our hospitals even made the news with a headline like: 'Staff are being tracked with chips.'"(I7, personnel communication, April 12, 2025)	Average
Mobility	Low	"Since UHF RFID technology is highly affected by environmental factors, and due to the large metallic load in our revolving door, it is very difficult for us to achieve 100% accuracy at every exit point."(I3, personnel communication, April 10, 2025)	Low
User Resistance and Adoption Barriers	Low	"There were two types of personnel within the hospital… We were having great difficulty getting public-sector personnel to use this product. Due to a lack of concern on their part, we encountered significant resistance."(I1, personnel communication, April 9, 2025) "I firmly believe that the fundamental issue that must be addressed is the human factor." (I2, personnel communication, April 10, 2025) "In my opinion, the human factor directly influences the success of the project."(I4, personnel communication, April 11, 2025) "Arguably, human factors represent the outermost framework and the area of greatest challenge at the outset."(I5, personnel communication, April 11, 2025) "Getting people to accept and use it, getting them to use it willingly and to feel that it is beneficial to their work, is, frankly, the most critical phase."(I6, personnel communication, April 11, 2025) "Therefore, the most important and most critical aspect to pay attention to is the human factor."(I7, personnel communication, April 12, 2025)	High

Practitioners nevertheless find the standard incomplete: "In my opinion, ISO/IEC 27001 focuses more on procedural information security; in the context of IoT, especially on the device security side, it may leave gaps" (I2, personal communication, April 10, 2025) and "I do not believe that ISO 27001 standards can be fully applied to IoT products in every sense" (I5, personal communication, April 11, 2025).

How governance is enacted further weakens its impact. Compliance work often becomes performative rather than protective; one manager observed, “Actually, it seems that hospitals are doing this not because they are fully aware and willing, but with a mindset of ‘we need to do it, so let’s do it’” (I3, personal communication, April 10, 2025). Governance responsibility also remains confined to IT: “Governance issues have remained within the IT departments of hospitals. It is not a topic that has spread across the entire hospital” (I5, personal communication, April 11, 2025). Strict privacy rules hinder essential integrations, “Even basic integrations are not being carried out due to data security concerns Even Active Directory integration is postponed by saying ‘let’s not activate it for now’” (I2, personal communication, April 10, 2025)while outdated certification pathways force ad-hoc workarounds: “We struggle to find a category to define the product while applying for CE certification . . . sometimes even two categories to avoid risk” (I3, personal communication, April 10, 2025).

Practitioners also underline a challenge scarcely covered in the literature: resistance from end-users. One project lead recalled, “There were two distinct types of staff in the hospital, and the team found it very difficult to persuade the public-sector personnel to use the product” (I1, personal communication, April 9, 2025). Another noted that, after installation, “Some systems remain unused because busy clinicians do not see an immediate benefit” (I4, personal communication, April 11, 2025). These statements show that adoption barriers arise from culture and workload, not from missing technical controls which explains why user-centered columns stand empty in the framework heat map.

Lastly, interviewees emphasize the importance of customizable and adaptive governance mechanisms. Rigid, static workflows are seen as inadequate in dynamic

clinical environments where technology, regulations, and organizational needs continually evolve. As one interviewee stated, “a customizable, evolvable workflow management structure, where we call the initial workflow a hypothesis… is very critical” (I2, personal communication, April 10, 2025). This insight reinforces the need for governance frameworks that treat operational processes as testable and revisable, encouraging iterative learning and enabling continuous alignment with real-world conditions.

Together these direct accounts clarify why strong controls reported in top-scoring frameworks rarely translate into daily practice user-adoption challenges persist ungoverned. The disconnect underscores the need for an integrated governance framework that pairs technical mechanisms with policies, incentives, and organization-wide change programs, a task taken up in the next research question.

5.4 RQ3. How can a new IoT governance framework be developed to address the challenges of IoT in healthcare?

This section introduces RQ3 by linking the previous literature and interview findings to the need for a new governance framework. The systematic review demonstrated that healthcare IoT reference architectures and governance models focus heavily on security, privacy, and regulatory compliance, but leave real-time performance and user resistance largely unaddressed. Interview data reinforce those gaps by showing that practitioners encounter widespread reluctance among clinical staff to adopt IoT tools. Even the most comprehensive frameworks, such as the six high scoring studies identified in the preceding chapter, do not provide mechanisms that resolve all the important challenge categories as whole especially user resistance is unaddressed. These gaps confirm that technical safeguards alone cannot ensure successful

deployment in complex clinical environments. A new framework must therefore preserve the proven strengths of existing security and compliance controls while adding targeted solutions for performance, efficiency, and stakeholder engagement. The following sections develop design principles and structural components that respond directly to these unmet needs.

5.4.1 Design principles derived from evidence

Empirical gaps must be distilled into explicit design principles that guide the new governance framework. Drawing on the Human–Organization–Technology fit (HOT-fit) model (Yusof et al., 2008), which stresses that value arises only when technical quality, organizational context and human capabilities are harmonized and on the Governance–Risk–Compliance (GRC) (Pratt, 2023; Rasmussen, 2006) paradigm, an operational strategy for aligning IT activity with business goals while managing risk and statutory obligations the following principles are proposed. These design principles for IoT governance in healthcare synthesize insights from earlier research questions, specifically, the architectural requirements identified in RQ1, the governance mechanisms analyzed in RQ2, and the practical realities shared through expert interviews.

First, the framework must uphold strong security and regulatory compliance mechanisms. As shown in RQ1, security and privacy dominate both reference architectures and practitioner concerns. RQ2 confirms this focus by revealing that nearly all governance models (29, 90%) embed provisions for security and compliance. Interview data further validate this emphasis, highlighting vulnerabilities in peripheral systems and the emergence of cybersecurity start-ups. These findings suggest that GRC functions, governance (policy clarity), risk

management (threat mitigation), and compliance (e.g., HIPAA/GDPR), should form the foundation of any healthcare IoT governance framework.

Second, ensuring real-time performance and operational efficiency requires explicit governance mechanisms. While latency and scalability are acknowledged in RQ1 and appear in several governance models from RQ2, neither stream presents consistent methods for sustaining performance under clinical conditions. Interviews reinforce this gap, linking latency directly to patient safety and logistical efficiency. In line with HOT-fit theory, governance should include system-quality metrics that align with frontline workflows, ensuring that technical performance translates into clinical utility.

Third, user engagement must be institutionalized as a governance priority. RQ2 reveals limited attention to user resistance and adoption, yet interviewees repeatedly cite behavioral obstacles that derail implementations, even when the underlying systems are technically sound. Embedding formal change management, training, and transparent communication practices within the governance framework addresses this gap and aligns with the human dimension of HOT-fit, supporting perceived usefulness and sustained adoption.

Finally, the governance framework should adopt a learning-oriented stance. RQ2 highlights that few existing models support iterative improvement or continuous monitoring. To address this, the proposed design should include dashboards and audit mechanisms that track residual risks, control effectiveness, and compliance drift. This shifts improvement from reactive fixes to a structured, evidence-based process, ensuring the framework evolves alongside clinical and technological changes.

These principles translate the evidence into actionable requirements that shape the structure and content of the proposed framework.

5.4.2 Structural overview of the proposed framework

The framework is presented as a three faced cube, shown in Figure 17 that integrates human, organization, and technology considerations while a central spine aligns governance, risk, and compliance processes. This geometric representation is isomorphic with the HOT-fit construct: each face depicts one subsystem who's fit with the others predicts health-ICT success. Running through the center is a GRC spine that couples board-level governance directives, real-time risk telemetry and automated compliance verification into a single assurance workflow (Pratt, 2023). Each face functions as an equal partner rather than a layered hierarchy so that decisions about people, organization, and technology remain synchronized from design through operation.

The human face emphasizes stakeholder education, change management, and ongoing user support, reflecting interview findings that staff resistance can derail projects even when systems are technically sound. By linking these routines to HOT-fit's user-satisfaction and system-use constructs, behavioral adoption becomes a first-class governance objective rather than a post-implementation after-thought.

The organization face sets out roles, accountability pathways, and performance metrics that convert abstract policy into clear operational duties.

The technology face houses reference architecture selections, security controls, and performance mechanisms that are configured to clinical requirements.

A side panel lists established standards such as ISO 27001, ISO 27799, and HL7 FHIR, instantiating the compliance arm of GRC; mapping these standards to

HOT-fit technology and organization dimensions provides traceable control lineage. The opposite panel offers a reference architecture selector that helps project teams choose among classical three-layer, edge oriented, multi-layer/service oriented, security-focused, or standards aligned models based on clinical latency needs, interoperability requirements, and available infrastructure. Together these elements form a coherent structure where each governance decision can be traced to a specific cube component, thereby ensuring that real time performance, efficiency, and user engagement receive the same formal attention as security and compliance.

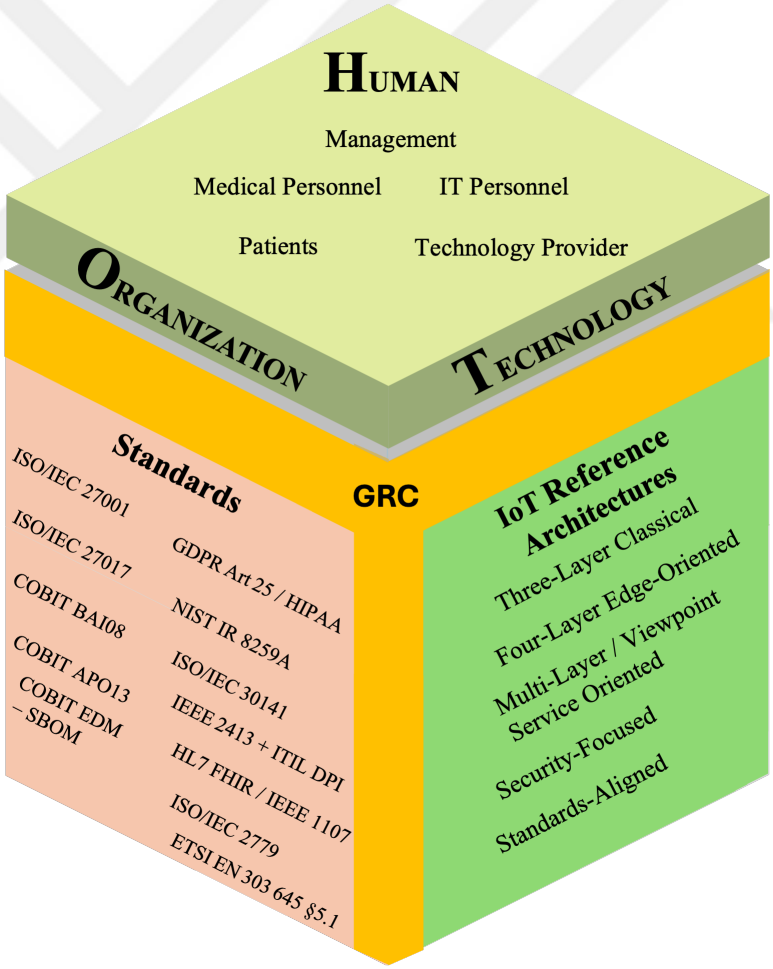

Figure 17. Govern-IoT-Health cube and the HOT-fit faces and the central GRC

5.4.3 Governance framework cycle

To operationalize the structure outlined in the proposed framework, a set of governance mechanisms has been developed and aligned with specific healthcare IoT challenges. These mechanisms represent concrete tools, protocols, and interventions that correspond to various project phases and governance objectives. Each mechanism was synthesized from gaps in the literature, practitioner insights, and regulatory expectations, ensuring both conceptual relevance and practical feasibility.

The governance framework cycles are organized around Deming's Plan Do Check Act model (PDCA), with the Check and Act stages merged into a single evaluative loop so that it will be called PDC. Govern-IoT-Health cube is extended with the three lifecycle stages determined as follows: "S1 PLAN", "S2 DO", and "S3 CHECK&ACT" (see Figure 18). The S1 PLAN phase sets objectives, allocates roles, and designs controls before any IoT-enabled healthcare service becomes operational. The S2 DO phase covers the implementation and daily operation of those controls while the system is live. The combined S3 Check and ACT phase brings systematic performance review together with immediate corrective action and continuous improvement, ensuring that insights from monitoring feed directly back into practice. This PDC logic accords with established governance literature, as ITIL links Service Design to Plan, Service Operation to Do, and Continual Service Improvement to the joint Check Act function, illustrating the cyclic nature of control (AXELOS, 2019).

COBIT embeds feedback through its monitor, evaluate, and assess domain while aligning planning and organization with forward-looking control, further showing how planning, execution, and feedback remain tightly integrated (ISACA, 2019). Standards like ISO/IEC 27001 follows the same rhythm by requiring organizations to design security controls, implement them, and subject them to audit-

driven review and corrective processes that sustain compliance (ISO/IEC, 2022a).By rooting IoT healthcare governance in this PDC cycle, the framework keeps pace with shifting risks and operational realities while maintaining a disciplined path for assurance and improvement.

Table 28 presents the controls that take effect before deployment assigned to S1 PLAN phase. In particular; software bill of material(SBOM) is a formal, machine-readable inventory of every software component packaged into a device's firmware or application. ETSI EN 303 645 (ETSI, 2020) recommend that IoT manufacturers document and make available a component list so operators can identify vulnerabilities and apply patches promptly. The "COBIT EDM – SBOM policy mandate" mechanism turns a high-level governance objective into a concrete control: no IoT device can be used without an ETSI-aligned SBOM that supports continuous risk monitoring and rapid remediation across the device life-cycle. These entries establish the governance baseline by setting accountability lines, selecting secure reference architectures, and embedding interoperability rules in the technical blueprint. Because the policies and patterns in this stage shape every downstream decision, anchoring them early prevents costly redesign and ensures that compliance obligations are understood before resources are committed.

Table 29 enumerates the mechanisms assigned to the S2 DO phase, which sustain governance while the IoT-enabled healthcare system is operational. Run-time enforcement controls such as the firmware-update gate that blocks any image with a Common Vulnerabilities and Exposures risk score above seven, mutual Transport Layer Security authentication between edge devices and the cloud, and tokenization of protected health information at ingress translate design objectives directly into live behavior. Continuous latency monitors, context-aware device posture checks, and

software-bill-of-materials banners embedded in the clinical user interface surface critical telemetry to clinicians without disrupting workflow. By consolidating these measures in the DO stage, the framework underscores their collective role in preserving performance, safety, security, and statutory conformance throughout routine clinical operation.

Table 30 collates the S3 CHECK & ACT mechanisms that transform operational data into systematic learning and corrective action. Automated instruments such as the two-second Software Bill of Material (SBOM) alert service, the TLS 1.3 conformance audit specified by ETSI EN 303 645 (ETSI, 2020), nightly FHIR (HL7 International, 2023) schema-drift tests, and the message-loss KPI set by IEEE 2413 (IEEE, 2020) feed high-frequency telemetry to governance teams, while monthly ISO 27001 control reviews and quarterly VPC gap scans mandated by GDPR and HIPAA provide deeper assurance snapshots. SIEM-based exfiltration indicators and the adoption-rate dashboard further reveal emerging security gaps and user-engagement trends. Findings from these monitors trigger root-cause analysis, targeted retraining, and policy revisions, so that each detection event informs an explicit improvement step. By coupling evidence generation with immediate remediation, the CHECK & ACT stage closes the governance loop and enables the framework to evolve in line with clinical practice, threat dynamics, and regulatory change.

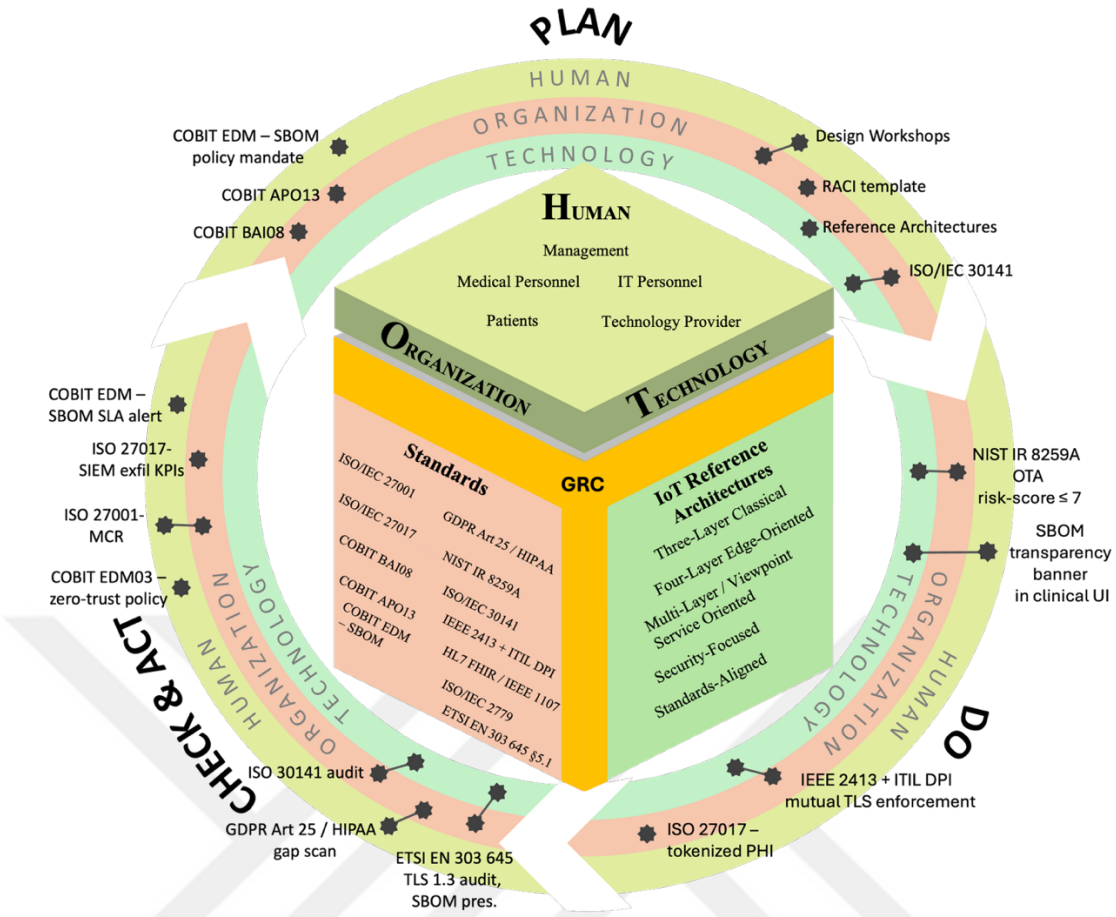

Figure 18. Govern-IoT-Health cube with PDC cycle

Presenting the mechanisms in three tables clarifies when each control activates and how its purpose shifts over time. Together the stages demonstrate that the proposed framework covers every identified challenge category now it matters most, linking early design intentions to day-to-day enforcement and long-term improvement.

Table 28. S1 PLAN Stage Mechanisms

Mechanism	Category	Cube Component	GRC	Summary	Challenge Categories
COBIT APO13 – vendor oversight & data-residency clauses	Control Standard	Organization	Governance, Compliance	Contract clause template that compels vendors to store protected health information within approved jurisdictions and provide regular security reports, aligned with COBIT APO13.	Security and Privacy, Data Management, Regulatory Compliance, Accountability and Transparency
ISO/IEC 30141 – architecture-control matrix sign-off	Control Standard	Organization-Technology	Governance, Compliance	Pre-go live checklist that maps each architecture element to its governing control and requires executive sign off under ISO 30141.	Security and Privacy, Interoperability/Standards, Scalability, Accountability and Transparency
COBIT BAI08 – vocabulary & interface catalogue	Control Standard	Organization-GRC Edge	Governance	Design artifact that establishes a shared vocabulary and catalogs all system interfaces to avoid semantic drift, aligned with COBIT BAI08.	Data Management, Interoperability/Standards, User Resistance and Adoption Barriers
Four-Layer Edge-Oriented Reference Architecture	Reference Architecture	Technology	Risk	Reference architecture that places compute resources at the edge to minimize latency and reduce backbone traffic.	Security and Privacy, Data Management, Scalability, Latency/Real-Time Performance
Multi-Layer Viewpoint Service-Oriented Reference Architecture	Reference Architecture	Technology	Risk	Service oriented reference architecture that separates concerns across multiple logical viewpoints to improve modularity and interoperability.	Security and Privacy, Data Management, Interoperability/Standards
Standards-Aligned Reference Architecture	Reference Architecture	Technology	Risk, Compliance	Reference architecture built directly on ISO 30141 and HL7 FHIR to maximize interoperability and regulatory alignment.	Interoperability/Standards, Regulatory Compliance, Accountability and Transparency
Security-Focused Reference Architecture	Reference Architecture	Technology	Risk, Compliance	Risk, Compliance	Reference architecture that layers encryption, blockchain audit, and identity management across the stack to maximize security.
Three-Layer Classical Reference Architecture	Reference Architecture	Technology	Risk	Traditional perception network application split that balances simplicity with integration requirements.	Security and Privacy, Data Management, Interoperability/Standards
Stakeholder RACI template for IoT-Health projects	Governance Artefact	Organization	Governance	Defines Responsible, Accountable, Consulted, Informed matrix across Board, Clinicians, IT, Vendors, Patients to clarify accountability before deployment	Accountability and Transparency
Participatory design workshops & UX heuristics checklist	Process	Human–Organization–Technology Human–Organization–Technology	Risk	Co-creation sessions with end-users + 10-item usability heuristics ensure early buy-in and mitigate adoption barriers	User Resistance and Adoption Barriers, Patient Acceptance and Awareness, Ethical Concerns
COBIT EDM – SBOM policy mandate	Control Standard	Human-GRC edge	Governance, Risk	Board-level policy that mandates a software bill of materials (SBOM) for every IoT device build.	Security and Privacy, Regulatory Compliance, Accountability and Transparency, Device Management

Table 29. S2 DO Stage Mechanisms

Mechanism	Category	Cube Component	GRC	Summary	Challenge Categories
NIST IR 8259A – OTA risk-score ≤ 7	Control Standard	Organization-Technology	Risk, Compliance	Run-time firmware update gate that blocks any over the air image with a Common Vulnerabilities and Exposures score higher than seven, following NIST 8259A guidance.	Security and Privacy, Device Management
SBOM transparency banner in clinical UI	Control Standard	Technology-Human	Risk, Compliance	Displays software-bill-of-materials & firmware provenance to build user trust in device updates (aligns with FDA pre-market guidance)	Security and Privacy, Accountability and Transparency, Device Management, User Resistance and Adoption Barriers
ISO 27017 – tokenized PHI	Control Standard	Organization	Compliance, Risk	Run-time cloud control that tokenizes protected health information on ingress in line with ISO 27017.	Security and Privacy, Data Management, Regulatory Compliance, Accountability and Transparency
IEEE 2413 + ITIL DPI – mutual TLS enforcement	Control Standard	Organization-Technology	Risk, Compliance	Run-time enforcement mechanism that ensures mutual TLS between edge nodes and cloud.	Security and Privacy, Interoperability/Standards, Latency/Real-Time Performance

5.4.4 Coverage validation

To enable a more precise comparison of challenge coverage across the top-performing governance frameworks and the Govern-IoT-Health proposal, a detailed mechanism count table is provided in Table 31. This table allows for a clearer assessment of how extensively each framework addresses the identified challenges. Figure 19 presents a heatmap that visualizes the number of mechanisms associated with each challenge category within each framework, offering a more nuanced understanding of their relative strengths and gaps.

Table 30. S3 CHECK and ACT Stage Mechanisms

Mechanism	Category	Cube Component	GRC	Summary	Challenge Categories
ETSI EN 303 645 §5.1 – TLS 1.3 audit, SBOM presence	Control Standard	Organization-Technology	Compliance, Risk	Periodic audit that verifies TLS 1.3 is enabled and confirms a software bill of materials is present for every device, as required by ETSI EN 303 645.	Security and Privacy, Regulatory Compliance, Accountability and Transparency, Device Management
GDPR Art 25 / HIPAA – quarterly VPC gap-scan	Control Standard	Organization-Human	Compliance, Risk	Privacy by design measure that runs automated vulnerability scans on virtual private cloud assets every quarter to maintain compliance with HIPAA and GDPR Article 25.	Security and Privacy, Data Management, Regulatory Compliance, Accountability and Transparency, Ethical Concerns
ISO 30141 audit – annual conformance test	Control Standard	Organization-Technology	Compliance, Governance	Independent audit that verifies system conformance to the ISO 30141 reference architecture once per year.	Security and Privacy, Interoperability/Standards, Regulatory Compliance, Accountability and Transparency
COBIT EDM03 – zero-trust policy & micro-segment map	Control Standard	Human-GRC edge	Governance, Risk	Zero trust network design that defines micro segmentation boundaries and governance metrics in accordance with COBIT EDM03.	Security and Privacy, Accountability and Transparency, Device Management
NIST SP 800-207 – continuous device-ID attestation	Control Standard	Organization-Technology	Risk	Runtime service that continuously polls device identity and posture to maintain zero trust compliance following NIST SP 800 207.	Security and Privacy, Accountability and Transparency, Device Management
ISO 27001 Annex A (2022) – monthly control review	Control Standard	Organization-Human	Governance, Compliance, Risk	Management review cycle that inspects key security controls and performance metrics every month under ISO 27001 Annex A.	Security and Privacy, Regulatory Compliance, Accountability and Transparency
HL7 FHIR / IEEE 11073 – schema-drift alarms; RCA	Control Standard	Technology	Compliance, Risk	Data validation pipeline that raises alarms when clinical data schemas drift from HL7 FHIR or IEEE 11073 standards and triggers root cause analysis.	Data Management, Interoperability/Standards, Accountability and Transparency
ISO 27799 – nightly FHIR conformance tests	Control Standard	Technology	Compliance, Risk	Automated nightly test suite that checks all FHIR endpoints against ISO 27799 privacy constraints.	Data Management, Interoperability/Standards, Regulatory Compliance, Accountability and Transparency
Adoption KPI dashboard (active-user %, training completion)	Metric	Human	Risk, Compliance	Monitors post-go-live user engagement, tracks mandatory HIPAA/GDPR training, feeds into continuous improvement	User Resistance and Adoption Barriers, Accountability and Transparency, Regulatory Compliance
Continuous training & feedback-loop programme	Process Improvement	Human-Organization	Governance, Risk	Quarterly refresher training, feedback surveys, and change-requests backlog close the loop on adoption issues	User Resistance and Adoption Barriers, Patient Acceptance and Awareness, Accountability and Transparency
COBIT EDM – SBOM 2 s alert SLA	Control Standard	Human/GRC edge	Governance, Risk	Monitoring metric that triggers an alert if SBOM mismatch is not reported within two seconds.	Security and Privacy, Regulatory Compliance, Accountability and Transparency, Device Management
ISO 27017 – Security Information and Event Management (SIEM) exfil KPIs	Control Standard	Organization	Compliance, Risk	Dashboard of exfiltration indicators from the SIEM that tracks anomalous PHI egress under ISO 27017.	Security and Privacy, Data Management, Regulatory Compliance, Accountability and Transparency
IEEE 2413 + ITIL DPI – message loss < 0.1 % KPI	Control Standard	Organization-Technology	Risk, Compliance	Loss KPI monitored and fed back for tuning under ITIL DPI.	Security and Privacy, Interoperability/Standards, Latency/Real-Time Performance

Table 31. Mechanisms Comparison of Govern-IoT-Health and Top Performing Governance Frameworks

Challenge	(Hasan et al., 2022)	(Dasgupta et al., 2019)	(Akkaoui et al., 2020)	(Sedrati et al., 2023)	(Chibuike et al., 2024)	(Aranha et al., 2019)	Govern-IoT-Health (GIH)
Security & Privacy	AES-128, secret sharing; Key-based pseudo-anonymity; anonymization; AVISPA	Encrypted transmission; Data anonymization	Symmetric encryption; RBAC, ECDSA auth; Data anonymization	Anonymization only; ABAC, IAM; Anonymization technologies	SSL/HL7/FHIR encryption; Data anonymization	Encrypted channels; eIDAS auth	Tokenization, TLS; Mutual TLS, RBAC; Tokenization & anonymization
Data Management	Off-chain storage, on-chain hash	End-to-end data lifecycle; Data classification, retention	IPFS off-chain + hashes	Five-stage process; Process includes monitoring	Data governance policies	—	Off-chain PHI tokenization; PDC cycle governance; Nightly FHIR schema tests
Interoperability/Standards	—	—	Blockchain as interop	Generic RA	HL7/FHIR advocated	HL7/FHIR & IHE; Modular EA	RA catalogue, FHIR tests; Blockchain + off-chain gateways; Modular RA
Scalability	Off-chain storage	—	Off-chain storage; Edge computing; Sharding / edge-mining pools	—	Edge computing noted	—	Off-chain tokenization & storage; Edge-oriented architecture; Parallel processing via RA options
Regulatory Compliance	Consent via smart contracts; Smart contract consent	Identify phase reviews regulations; Records explicit consent	HIPAA, GDPR; Smart contracts require consent; Off-chain identity HCA	Regulatory alignment process; Ethics as strategic input	Emphasizes GDPR; Stakeholder collaboration	EU NIS & GDPR	HIPAA/GDPR policies; Consent & SBOM policies; Ethics incorporated in HOT-fit
Accountability & Transparency	Blockchain immutability; Owner controlled policies	Corporate data governance	Smart-contract logs; Smart-contract consent	Ethereum irreversible ledger; RACI	Blockchain auditability; Transparent consent	—	Immutable logs & SBOM; RACI templates; Consent management & dashboards
Latency Real-Time	Prioritizes emergency traffic	—	Edge computing; Adjustable block period	—	Edge/fog computing advocated	—	Latency SLA & QoS monitors; Edge computing RA; Latency dash. &probes
Device Management	QoS & decision ability assessment	—	Device auth & firmware verification	Device classification process	—	RAMI asset layer	OTA gates, mutual TLS; Lifecycle & attestation controls; Device registry-asset map.
Mobility	WBAN sensors	—	Personal health devices	—	—	mHealth; Mobile med. devices; Remote mon.	—
Energy Efficiency	—	—	PoA consensus; Edge reduces energy	Acknowledges energy study	—	—	—
Ethical Concerns	Full control & consent	Consent mechanism	—	Ethics in design	Ethical gov.; Balance privacy-innovation	—	Consent cont. in GRC; Ethics mapped to HOT-fit; Privacy & innov. balance
Patient Accept. Awareness	Patient-centric design	Transparent consent;	Ownership via smart contracts; Data anon.	Transparency-control	—	—	Participatory design; Adoption KPI & training; Tokenization & user control
User Resistance - Adoption Barriers	—	—	—	—	Continuous education	Security embedded at design stage	Adoption training program; Participatory design & UX workshops; Built-in security & zero-trust

A consistent blue band across categories such as Security and Privacy, Data Management, and Accountability and Transparency highlights their prominence across both existing literature and the proposed model. In contrast, sporadic coverage is evident for latency, scalability, device management, ethical concerns, and user resistance and adoption barriers. Some of these areas show mechanisms in only a few frameworks, including P35 and P55 providing limited but noteworthy coverage. The Govern-IoT-Health column stands out with near-complete challenge addressing, showing blue for nearly all categories. The only exceptions, “Energy Efficiency” and “Mobility”, remain unaddressed, aligning with their lower prioritization in both the reviewed literature and expert interviews.

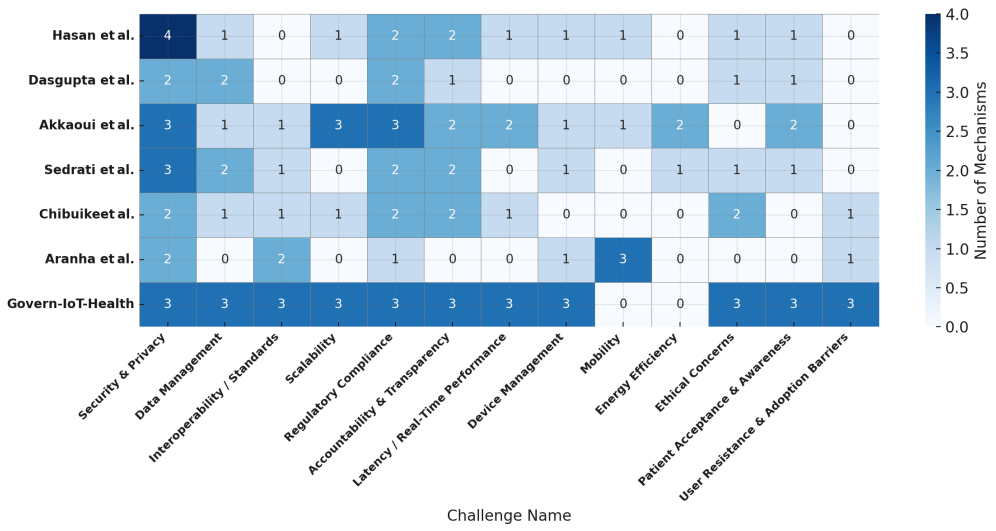

Figure 19. Top-performing frameworks and Govern-IoT-Health challenge mechanism counts heatmap

The heat-map thus provides the first empirical check on the mechanisms, by visual inspection, Govern-IoT-Health eliminates nearly all gaps that persist across existing frameworks. A second, more granular overlay analysis mapped every mechanism to the thirteen challenge categories and confirmed that each is now addressed by at least one dedicated control, with the same two exceptions noted

above. Security and privacy measures are distributed across all three life-cycle stages; latency controls cluster in the DO phase, where their effect on clinical decision speed is greatest; adoption barriers are tackled during Design through participatory workshops and revisited in CHECK&ACT by way of continuous training.

To triangulate these findings, interview excerpts were revisited. Practitioners repeatedly highlighted user resistance, latency, and interoperability as operational pain points; the governance framework cycle now links each of these concerns to multiple mechanisms, for example, an adoption KPI dashboard that feeds quantitative engagement data into governance reviews, edge-oriented architectural patterns that mitigate time-critical delays, and schema-drift alarms that preserve interoperable data flows. The alignment between practitioner testimony and the governance framework cycle confirms that the framework answers real-world needs rather than merely filling theoretical gaps.

Finally, a judgment-based tiering evaluated the depth of support for each challenge. Categories buttressed by several well-integrated mechanisms were graded High, those covered by single but explicit controls were graded “Moderate”, and those touched only marginally remained Low. Table 32 records the results: Convergent strengths retain their “High” status; latent gaps such as accountability and device management rise to “High” through new audit trails and lifecycle registries; emergent practitioner concerns like user resistance and latency advance to “Moderate” or “High” depending on the density of controls. Overall, Govern-IoT-Health consolidates the convergent priorities identified in both evidence strands, amplifies latent academic concerns, and embeds emergent practitioner needs, thereby

satisfying RQ3's requirement for a governance framework that is both comprehensive and operationally relevant.

The RQ3 analysis demonstrates that while existing healthcare-IoT governance frameworks excel in traditional domains such as "Security and Privacy" and "Regulatory Compliance", they provide only fragmented or negligible guidance on "Interoperability and Standards", "Latency and Real-Time Performance", "User Resistance", and "Device Management", gaps that practitioners highlighted as decisive barriers to safe and effective deployment. By synthesizing these empirical deficiencies into explicit design principles and mapping them to lifecycle-aligned mechanisms, the Govern-IoT-Health framework transforms isolated best practices into a coherent, stage-sensitive system of controls. The heat-map (see Figure 19) shows that the proposal converts most of the white spaces left by the six benchmark studies into comprehensive coverage, and the tiered evaluation in Table 32 confirms a decisive shift of previously under-served challenges from "Low" or "Moderate" to "High" assurance levels. These results indicate that Govern-IoT-Health not only consolidates convergent academic and practitioner priorities but also operationalizes latent and emergent concerns, thereby delivering the integrative governance architecture required for resilient, user-centered and performance-capable IoT adoption in complex clinical environments.

Table 32. SLR, Interviews, and Govern-IoT-Health Challenge Coverage Tiers

Challenge	SLR Tier	Interview Tier	Govern-IoT-Health Tier
Security and Privacy	High	High	High
Data Management	High	Moderate	High
Interoperability / Standards	High	High	High
Scalability	High	Moderate	High
Regulatory Compliance	High	High	High
Accountability and Transparency	Moderate	High	High
Latency / Real-Time Performance	Moderate	Moderate	Moderate
Energy Efficiency	Moderate	Low	Low
Patient Acceptance and Awareness	Moderate	Low	Moderate
Ethical Concerns	Moderate	Low	Moderate
Device Management	Moderate	Moderate	High
Mobility	Low	Low	Low
User Resistance and Adoption Barriers	Low	High	High

5.4.5 Sample case study: Implementing a wearable-sensor early-warning system in a hospital

This scenario shows how the Govern-IoT-Health cube and its PDC stages steer deployment. High-risk post-surgical patients are equipped with skin-patch sensors that stream heart-rate and SpO_2 to the EMR and raise bedside alerts when readings deteriorate.

Table 33 captures Stage S1 PLAN (months 0–4), the pre-deployment phase in which governance foundations are laid and stakeholders aligned before any IoT service goes live. Actions span the cube's organizational, technological, and human facets, all anchored to the GRC spine. Each step couples a concrete mechanism—policy mandates, reference architectures, participatory workshops—to a specific challenge (regulatory compliance, 200ms latency, alarm fatigue). The result is a launch-ready blueprint for smooth transition into later operational and feedback stages.

Table 33. Stage S1 PLAN - Pre-deployment

Step	Governance action	Cube facet(s)	Key mechanism	Purpose / challenge addressed
1.1	Board mandate & scope definition	Organization → GRC spine	COBIT EDM – SBOM policy mandate	Sets top-level security expectation; anchors vendor selection in verifiable software provenance.
1.2	Vendor RFP & contract clauses	Organization	COBIT APO13 – vendor oversight & data-residency clauses	Ensures PHI remains in approved jurisdictions; obliges quarterly security reporting.
1.3	Reference-architecture choice	Technology	Four-Layer Edge-Oriented RA	Places analytics gateway on the ward to meet 200ms alert-latency requirement.
1.4	Architecture–control matrix sign-off	Org + Tech	ISO/IEC 30141 control matrix	Maps every layer of the chosen RA to a control in ISO 27001 / GDPR Art 25.
1.5	Stakeholder alignment workshop	Human + Organization	Participatory design sessions & UX-heuristics checklist	Surfaces clinician concerns about alarm fatigue; co-designs color-coded alerts.
1.6	Accountability mapping	Organization	Stakeholder RACI template	Clarifies who is Responsible (Ward IT), Accountable (CMIO), Consulted (Nursing), Informed (Patients).

By month 4 the project owns an executive-approved policy stack, a latency-tuned architecture, and documented roles—de-risking procurement and priming staff for change.

Table 34 shows Stage S2 DO (months 5–10), when the planned controls run in production. Mechanisms spanning human, organizational, and technological facets secure onboarding, shield data, monitor the 200ms SLA, and surface firmware hashes, turning policy into day-to-day safety and trust. This step in the P-D-C cycle renders governance measurable and enforceable across clinical systems.

The ward goes live in month 7; by month 10, 95 % of target patients are connected, no unauthorized firmware is detected, and median alert latency is 140ms.

Table 34. Stage S2 DO - Deployment & Operation

Step	Live control or process	Cube facet(s)	Mechanism invoked	Operational effect
2.1	Secure device onboarding	Organization + Technology	IEEE 2413 + ITIL DPI mutual-TLS enforcement	Rejects any sensor that fails x.509 attestation; prevents rogue devices.
2.2	Firmware-update gate	Technology	NIST IR 8259A – OTA risk-score ≤ 7	Blocks patches with unpatched CVEs; maintains software hygiene without manual review.
2.3	Live SBOM transparency banner	Human + Technology	SBOM UI banner	Displays current firmware hash in EMR; builds clinician trust in automated updates.
2.4	PHI tokenization on ingress	Organization	ISO 27017 – tokenized PHI	De-identifies vitals before cloud analytics; satisfies GDPR/HIPAA at run time.
2.5	Edge latency monitor	Technology	(custom) REST-endpoint probe, 200 ms SLA	Logs round-trip delay; feeds metric into DO dashboard for proactive scaling.

Table 35 details Stage S3 CHECK & ACT, launched in month 7 and run continuously to convert live evidence into corrective action. Audit routines, telemetry, and user metrics span all HOT-fit facets, verifying that controls adapt to shifting clinical and technical demands. Feedback channels—nightly conformance tests, TLS audits, SBOM alerts, and adoption dashboards—spot drift and trigger fixes via patches, policy tweaks, or retraining, embedding governance as an evolving practice rather than a static checklist.

Within the first review cycle every audit finding is closed, night-shift usage rises to 93 %, and rapid-response calls fall 25 %, confirming that technical, organizational, and human controls work in concert.

Table 35. Stage S3 CHECK & ACT - Assurance & Improvement

Step	Evidence source	Cube facet(s)	Mechanism	Action & learning loop
3.1	Nightly conformance tests	Organization + Technology	ISO 27799 – nightly FHIR tests	Failures auto-generate Jira tickets; two mapping errors fixed in week 1.
3.2	TLS 1.3 compliance audit	Organization + Technology	ETSI EN 303 645 §5.1 audit	Annual audit finds 4 devices on legacy TLS 1.2; vendor patch forced within 24 h.
3.3	Real-time SBOM alert (≤ 2 s)	Human-GRC edge	COBIT EDM – SBOM alert SLA	One alert fires in month 12; root cause traced to staging repo mis-sync, policy updated.
3.4	Adoption KPI dashboard	Human	Active-user %, training completion	Reveals night-shift nurses lag at 70 % usage; triggers extra on-floor coaching.
3.5	Monthly ISO 27001 Annex A review	Organization -Human	ISO 27001 Annex A cycle	Residual-risk score drops from 14 → 9 after token-rotation frequency doubled.

The case study confirms that Govern-IoT-Health meets all RQ3 goals. End-to-end security and compliance flow from SBOM mandates in PLAN, through OTA firmware gates in DO, to multi-layer audits in CHECK & ACT. Edge-based architecture and latency probes keep alerts under 200ms. Participatory design, interface transparency, and KPI coaching turn early skepticism into sustained use. Continuous improvement—via automated tests and monthly reviews—builds an evidence trail for board-level dashboards. Overall, the framework unites policy, technology, and human factors across the P-D-C cycle, delivering quantifiable clinical gains while staying aligned with international standards.

CHAPTER 6

DISCUSSION

This chapter situates the study's findings within the wider healthcare-IoT discourse. Evidence from a 76-paper review and seven hospital interviews shows that hospitals need governance solutions that link reference architecture, risk policy and change-management, not stand-alone technical controls. Govern-IoT-Health, devised for RQ3, meets that need through a three-faced cube that aligns Human, Organization and Technology decisions around a Governance-Risk-Compliance spine, adds edge-latency safeguards, SBOM-based device registers and adoption KPIs, and embeds HIPAA/GDPR duties. The discussion revisits each research question, compares results with prior work, and outlines practical contributions, limitations and avenues for future research.

6.1 Reflection on RQ1

The combined evidence underscores that technical performance in healthcare IoT is not an abstract engineering target but a direct determinant of patient safety. Practitioner accounts link specific architectural weaknesses such as location-tracking failures and unverified device integrations to scenarios with lethal potential (I2, personal communication, April 10, 2025). These observations resonate with systematic-review findings that place security, data management, interoperability, scalability, and latency at the center of architectural design (Nguyen et al., 2020; Bodkhe et al., 2020; Dang et al., 2021). The convergence implies that, within clinical settings, architectural robustness functions as a form of risk control comparable to traditional medical safety protocols.

Closer comparison also reveals important asymmetries between scholarly models and operational realities. While the literature increasingly proposes edge-oriented or security-focused blueprints to mitigate latency and cyber-threats (Firouzi et al., 2022; Scalco et al., 2021; Sittón-Candanedo et al., 2019), interview data highlight context constraints such as signal obstruction by metal doors that can nullify performance gains achieved in the lab (I3, personal communication, April 10, 2025). Such discrepancies suggest that real-world clinical environments impose a layer of complexity inadequately captured by many published designs. Consequently, the absence of an agreed-upon, context-sensitive standard leaves hospitals balancing incompatible design logics from multiple vendors, amplifying both procurement risk and integration cost (I1, personal communication, April 9, 2025; I5, personal communication, April 11, 2025).

The architectural diversity catalogued in forty-four studies, including Three-Layer Classical, Four-Layer Edge-Oriented, Multi-Layer Service-Oriented, Security-Focused, and Standards-Aligned variants, illustrates an evolutionary shift from minimalist stacks toward hybrid, problem-specific solutions (Santos et al., 2016; Elgammal & Krämer, 2021; Talaminos-Barroso et al., 2022). Yet the piecemeal emergence of these models reveals a reactive posture. Each new layer or overlay typically addresses an isolated vulnerability rather than delivering holistic assurance. This fragmentation explains persistent practitioner frustration over unclear upgrade pathways and uneven governance coverage, particularly where architectural choices must satisfy overlapping regulatory, operational, and human-factor demands.

Taken together, these interpretations affirm that healthcare IoT architectures must be conceived as integrated socio-technical systems. Technical layers need to be explicitly mapped to clinical workflows, environmental constraints, and legal

mandates. Otherwise, even the most sophisticated blueprint remains vulnerable to unforeseen failure modes. Current scholarship provides valuable building blocks, including edge computing for latency, blockchain for data integrity, and formal standards for interoperability. However, the evidence indicates that only cohesive and context-aware assemblies of these elements can meet the sector's life-critical expectations.

6.2 Reflection on RQ2

Review findings show that healthcare-IoT governance research concentrates on a small cluster of technical and policy concerns. Security and privacy appear in nearly all frameworks, while data management and, more recently, accountability and transparency also receive substantial attention (Hasselgren et al., 2021; Scalco et al., 2021). Performance-oriented topics such as latency and energy efficiency, together with user-centered issues like resistance and adoption barriers, remain under-studied in the academic discourse. This focus suggests that, within the literature, governance is conceived chiefly as a safeguard for data protection and regulatory compliance rather than as a holistic instrument for operational success.

Interview evidence paints a markedly different picture. Practitioners emphasize socio-technical obstacles that outweigh purely technical ones. Staff resistance is common in resource-constrained public hospitals, where heavy workloads push IoT systems down the priority list (I1, personal communication, April 9, 2025; I3, personal communication, April 1, 2025). Organizational immaturity further complicates implementation, with vague project scoping and disconnects between procurement teams and clinical users (I4, personal communication, April 11, 2025; I5, personal communication, April 11, 2025). Poorly

integrated technology can also produce unintended effects such as alarm fatigue, prompting clinicians to ignore or disable safety alerts (I2, personal communication, April 10, 2025). These accounts reposition human and organizational factors as the principal barriers to adoption, elevating them from secondary considerations in the literature to critical determinants of success.

The gap between scholarship and practice becomes clearer when the range of proposed governance tools is compared with those actually employed. Although studies advocate diverse models, including bespoke frameworks like 4I or established standards such as COBIT and ISO 27001 (Dasgupta et al., 2019; Kakkar, 2019; Singh and Sharma, 2021; Sedrati et al., 2023), practitioners rely almost exclusively on ISO 27001, often as a contractual requirement rather than a strategic choice (I1, personal communication, April 9 2025; I4, personal communication, April 11, 2025; I7, personal communication, April 12, 2025). Broader frameworks such as COBIT have little penetration in healthcare settings; one engineer had never encountered the term before the interview (I2, personal communication, April 10, 2025). Furthermore, ISO 27001 is viewed as too generic and process-centric to address hardware-focused risks, leaving a governance vacuum around device security (I2, personal communication, April 10, 2025; I5, personal communication, April 11, 2025).

Implementation practices further weaken the efficacy of these frameworks. Several interviewees described compliance as a box-ticking exercise aimed at acquiring certificates rather than mitigating risk (I3, personal communication, April 10, 2025; I6, personal communication, April 11, 2025). Governance responsibilities often remain siloed within IT departments, failing to reach clinical or operational units that interact with IoT devices daily (I5, personal communication, April 11,

2025). Coupled with lagging certification pathways for innovative hybrid devices, this culture of superficial compliance leaves critical security, performance, and adoption issues unresolved (I3, personal communication, April 10, 2025). The divergence between theoretical emphasis and operational need therefore exposes a persistent governance gap: academic frameworks solve problems that, while important, do not fully correspond to the challenges practitioners confront in real healthcare environments.

6.3 RQ3 and the Govern-IoT-Health framework

The benchmark literature reaches a firm consensus on four foundational domains: Security and Privacy, Data Management, Regulatory Compliance, and Accountability and Transparency. Each of the six top-performing frameworks embeds cryptographic safeguards, immutable ledgers, or role-based controls to protect data and produce audit evidence (Hasan et al., 2022; Dasgupta et al., 2019; Akkaoui et al., 2020; Sedrati et al., 2023; Chibuike et al., 2024; Aranha et al., 2019). Govern-IoT-Health deliberately preserves this secure-compliance core, matching the literature's established strengths and thereby ensuring continuity with accepted best practice.

Important divergences become visible when the same sources are compared against practitioner priorities. Only two of the six studies report quantitative latency results, and neither link those figures to operational governance levers such as alert service-level thresholds. Device management appears only as isolated registration or update checks, while structured approaches to staff adoption and alarm fatigue are almost entirely absent. These omissions contrast sharply with interview evidence that identifies latency, device management, and user resistance as decisive barriers to safe

deployment (I2, personal communication, April 10, 2025; I5, personal communication, April 11, 2025).

Govern-IoT-Health addresses the identified gaps by integrating edge-oriented architectural options, a two-second alert threshold, continuous device-identity attestation, software-bill-of-materials transparency, participatory design workshops, adoption key-performance indicators, and quarterly training loops. Through these mechanisms the framework extends governance beyond data protection to encompass real-time performance, asset stewardship, and behavioral uptake. Re-interpreted through the Human–Organization–Technology fit lens, earlier frameworks concentrate their effort in the technology corner, whereas Govern-IoT-Health distributes controls evenly across all three facets, achieving the balance recommended by Yusof et al. (2008). Examined from a Governance–Risk–Compliance perspective, the framework couples board-level directives to live risk telemetry and automated compliance evidence, fulfilling the continuous-assurance ideal articulated by Pratt (2023).

Coverage analysis confirms the clear added value of Govern-IoT-Health. As shown in Table 31 and visualized in Figure 19, Govern-IoT-Health substantially enhances existing IoT governance frameworks. According to the comparative analysis, Govern-IoT-Health aligns with fundamental governance principles emphasized in prior studies, particularly those regarding security and privacy, data management, and regulatory compliance (Hasan et al., 2022; Dasgupta et al., 2019; Akkaoui et al., 2020). However, it notably diverges by introducing comprehensive, real-time operational controls explicitly addressing latency, device management, and user resistance areas previously identified as inadequately covered or merely

superficially addressed in existing governance frameworks (Sedrati et al., 2023; Chibuike et al., 2024; Aranha et al., 2019).

Specifically, while earlier studies primarily relied on theoretical or generalized strategies, Govern-IoT-Health uniquely integrates participatory co-design workshops to address practical adoption challenges directly, such as workload pressures leading to underutilization of IoT systems. This user-centered approach is supported by real-time adoption dashboards that actively detect and mitigate issues like alarm fatigue, employing targeted retraining instead of ad-hoc corrective measures. Further enhancing its distinctiveness, the framework introduces quarterly feedback loops, systematically aligning governance strategies with frontline clinician perceptions and thereby directly mitigating resistance or skepticism—critical elements scarcely addressed by prior research.

Nevertheless, the analysis also highlights persistent gaps related to energy efficiency and mobility, consistent with their lower perceived importance in both existing literature and practitioner insights. Despite these limitations, the innovative integration of performance metrics, provenance tracking, and socio-technical adjustments positions Govern-IoT-Health as superior, effectively bridging significant practical gaps that prior studies have consistently overlooked. Consequently, Govern-IoT-Health represents an advanced governance framework capable of effectively translating theoretical governance concepts into tangible, practical improvements within IoT-enabled healthcare environments.

Coverage analysis confirms the added value of Govern-IoT-Health. Figure 19 lifts 11 of 13 challenge categories to full coverage, raising latency, device management, and especially user resistance from low or moderate assurance in the benchmark literature to high assurance in the proposed scheme. User resistance

receives explicit, multi-layer attention: participatory co-design workshops surface workload pressures that previously led staff to bypass IoT tools (I1, personal communication, April 9, 2025; I3, personal communication, April 10 2025); adoption dashboards track real-time utilization so that alarm-fatigue patterns, which once prompted clinicians to silence alerts, trigger targeted retraining rather than ad-hoc fixes (I2, personal communication, April 10 2025); quarterly feedback loops align governance metrics with frontline perceptions of value, addressing the skepticism reported when busy clinicians saw no immediate benefit in new systems (I4, personal communication, April 11, 2025). Energy efficiency and mobility remain lightly served, reflecting their lower salience in both the systematic review and practitioner interviews, yet the integration of performance, provenance, and human-factor controls closes the principal governance gaps left by the benchmark studies. In sum, Govern-IoT-Health converges with the literature on secure-compliance fundamentals while diverging constructively by embedding real-time, device, and socio-technical mechanisms that align governance with the operational realities of connected clinical care.

The results show that while existing architectures and governance models already deliver mature safeguards for security, privacy, and regulatory compliance, they leave critical deficits in real-time performance, device management, accountability, and most importantly user resistance. Govern-IoT-Health was therefore conceived to preserve those well-established controls yet infuse them with mechanisms that tackle latency thresholds, trace operational accountability, and embed change-management routines that clinicians will adopt. The discussion that follows interprets how this integrated cube-and-framework-cycle design meets those needs by systematically comparing its coverage and operating logic with six top-

performing frameworks identified in the systematic review, thereby clarifying both its incremental and novel contributions to healthcare-IoT governance.

6.4 Theoretical contributions

The integration of HOT-fit with a Governance–Risk–Compliance loop offers a limited contribution to the theory. First, it repurposes HOT-fit, which is usually applied as a diagnostic lens after implementation, into a forward-looking design scaffold that assigns concrete governance artefacts to the human, organizational, and technological dimensions at each life-cycle stage. Second, embedding a continuous GRC telemetry spine inside the cube places risk sensing and compliance evidence within the same socio-technical matrix, showing that organizational governance and technical assurance can be coordinated through one set of controls rather than treated as parallel streams. Finally, by treating user resistance as a formal governance object with explicit accountability and performance indicators, the framework demonstrates that behavioral adoption can be monitored alongside encryption strength or latency budgets, a modest but useful step toward integrating human factors into routine assurance practice.

6.5 Practical implications

The interview results provide additional evidence on how Govern-IoT-Health aligns with day-to-day pain-points reported by clinicians and technology managers. One frequently coded excerpt shows an operations manager lamenting that “public-sector personnel could not be persuaded to use the product until extra training sessions were scheduled, and workload relief was negotiated” (I1, personal communication, April 9, 2025; I2, personal communication, April 10, 2025; I6, personal communication,

April 11, 2025). Because the framework embeds participatory design workshops before deployment and couples quarterly refresher training with an adoption-KPI dashboard, it offers a direct remedy for exactly that form of disengagement. Another cluster of entries records frustration over the “lack of clear IoT standards” that leaves procurement teams “quite uncertain which vendor to trust or which certificate to demand” (I1, personal communication, April 9, 2025). The reference-architecture selector and standards mapping panel in Govern-IoT-Health transform that uncertainty into a repeatable evaluation path, giving buyers a standards-aligned checklist that can be inserted into tender documents without bespoke engineering effort.

Compliance practice emerges as a third weak spot: several respondents describe regulatory audits as “a box-ticking exercise that satisfies paper requirements but does little for real security” (I3, personal communication, April 10, 2025). The framework counters this habit by binding every policy to measurable controls, such as mandatory software-bill-of-materials disclosure and a two-second alert service-level threshold, both of which feed automated reports into the governance dashboard; auditors therefore review live risk metrics rather than paperwork. Interviewees also highlighted device-related hazards: one practitioner recalled a psychiatric patient leaving a secure area after a location tag failed, while another worried about “devices whose calibration date has already expired” (I2, personal communication, April 10, 2025). Govern-IoT-Health mitigates these risks through continuous identity attestation, firmware-risk scoring, and an asset registry that links each device to its calibration and maintenance record, thereby closing the governance gap around lifecycle accountability. Finally, project-management misalignment surfaced in multiple responses, including complaints that IoT alarms were added without clear

clinical goals and that project methodologies varied wildly across departments (I3, personal communication, April 10, 2025). By staging mechanisms across Design-and-Build, Operate-and-Monitor, and Assure-and-Improve phases, the framework imposes a common rhythm that synchronizes technical tasks with clinical objectives and continuous feedback loops. Taken together, these mappings illustrate how the framework cycle's controls translate interview findings into actionable governance artefacts that improve adoption, procurement certainty, audit integrity, device safety, and project coherence.

6.6 Limitations and directions for future research

While the Govern-IoT-Health framework addresses several persistent gaps in healthcare IoT governance, it is important to acknowledge its contextual and methodological limitations. First, the empirical basis of the framework is drawn entirely from seven semi-structured interviews conducted in technology providers and healthcare facility managers in Turkiye. As a result, the findings may not fully reflect the governance needs of other regions, such as low-resource settings in Sub-Saharan Africa or digitally mature systems in the United States. Regulatory interpretations, infrastructural capabilities, and adoption pressures vary considerably across jurisdictions, and further fieldwork will be necessary to confirm the framework's global relevance. In addition, most respondents were mid-level managers or senior technicians; the perspectives of patients and frontline nurses appear only indirectly through anecdotal remarks. Future studies should triangulate these insights with direct patient and healthcare personnel engagement to validate the framework's global applicability and user-centric promises.

Second, the coverage validation conducted in this study is based on binary inclusion logic except top performing governance framework analysis, each mechanism is either present or absent for a given challenge category. While this provides clarity on breadth, it does not account for depth, criticality, or operational cost. Future work could expand the heat-map weighted scoring model that captures the relative implementation burden, stakeholder value, and resilience contribution of each control.

Third, although the proposed mechanisms are grounded in literature, international standards, and practitioner testimony, the framework has not yet been piloted in a live healthcare setting. It remains a conceptual artefact, and its implementation effects on adoption, alert responsiveness, and compliance cost have not been empirically measured. A logical next step is a longitudinal study that deploys the framework within a high-acuity department, such as emergency or intensive care, where real-time performance and device governance are particularly critical. Such a pilot would not only verify the viability of specific controls, such as the two-second alert SLA and adoption KPI dashboard but would also provide insight into how the three life-cycle stages interact in dynamic clinical environments. Testing the framework in this way would help refine its structure and clarify whether the two low-coverage categories, energy efficiency and mobility, should be elevated to higher priority status in future iterations.

CHAPTER 7

CONCLUSION

This study set out to examine why healthcare environments need dedicated Internet of Things reference architectures, to identify the challenges that shape those environments, to evaluate the adequacy of existing governance frameworks, and finally to design a more complete alternative. The SLR plus seven practitioner interviews proved effective: it revealed convergent priorities around security, privacy, interoperability and regulatory compliance, but also exposed neglected domains such as device lifecycle control, latency management and user resistance. The Govern-IoT-Health framework was developed to close those gaps.

A concise recap of the three research questions demonstrates the trajectory of the inquiry. Research Question 1 confirmed that generic IoT blueprints are insufficient for clinical settings because they underplay strict latency thresholds, multi-jurisdictional privacy duties and human-factor obstacles. Five architecture families were determined, yet each left at least one blind spot in performance or adoption. Research Question 2 showed that prevailing governance frameworks, chiefly ISO 27001, COBIT, and sector-agnostic IoT models, secure data well and document compliance obligations, but they supply limited guidance on real-time assurance, device oversight and socio-technical change management. Research Question 3 produced the Govern-IoT-Health proposal, a cube that unites human, organization and technology decisions with a Governance-Risk-Compliance telemetry spine and allocates eleven of the thirteen identified challenge categories to concrete mechanisms across design, operation and improvement stages.

The theoretical contribution is incremental. By turning HOT-fit from a post-hoc diagnostic into a prescriptive scaffold and weaving a continuous Governance-Risk-Compliance loop through that scaffold, the framework demonstrates how socio-technical alignment and risk assurance can be co-engineered rather than treated as parallel concerns.

Practical value is clearer. Interviewees described stalled deployments that required additional training and workload relief before clinicians embraced new devices. They also reported procurement stalemates caused by the absence of a recognized IoT standard and compliance audits that reduced security to a "box-ticking exercise". By embedding participatory design workshops, a standards-mapping panel, adoption dashboards and live SBOM and alert-latency metrics, Govern-IoT-Health converts those frustrations into accountable, measurable routines that link frontline practice to board-level oversight.

Limitations temper these claims. The empirical base consists of seven interviews conducted in Turkiye; the framework's relevance to low-resource or highly digitized jurisdictions therefore remains to be tested. The binary heat-map used for coverage validation privileges breadth over depth, and the framework cycle has not yet been piloted in a live ward, so its impact on clinical outcomes and compliance cost is still hypothetical. Future work should carry out longitudinal pilots in high-acuity units, expand the evaluation to energy efficiency and mobility, and develop a weighted scoring model that captures implementation burden and risk criticality.

In closing, the study demonstrates that hospitals require more than isolated technical safeguards; they need an integrative governance architecture that aligns human, organizational and technological decisions with continuous risk telemetry.

Govern-IoT-Health offers such an architecture. By translating latent academic concerns and emergent practitioner needs into a stage-sensitive mechanisms, it provides a practicable path toward secure, performance-capable and user-centered IoT adoption in complex clinical environments.

APPENDIX A

PRIMARY PAPERS

Study ID	Related RQs	Title	Reference	Document Type	Online Database/Publisher	Summary	Theme	Methodology	Research Strategy	Data Collection Methods	Country
P1	RQ1	6G-IoT Framework for Sustainable Smart City: Vision and Challenges	(Mishra & Singh, 2023)	Book Section	Springer Nature	The chapter describes the evolution from 1G to 6G, addresses core 6G requirements, and proposes a six-layer 6G-IoT reference architecture aimed at sustainable smart cities. It highlights enabling technologies like AI, terahertz communication, and edge computing, as well as challenges such as security, privacy, interoperability, and reliability.	Reference Architecture	Qualitative	Conceptual Study	Literature review	
P2	RQ1, RQ2	A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks	(Hasan et al., 2022)	Journal Article	Computer Networks (Elsevier)	The paper introduces a decentralized model combining SDN-based WBANs with blockchain to manage patient-centric data sharing. It outlines protocols for secure data storage, encryption, and distributed access control via smart contracts. Formal security analyses (AVISPA) confirm resilience to tampering and unauthorized access.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study, Single case study	Case study, Experiment	
P3	RQ2	A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems	(Dasgupta et al., 2019)	Conference Paper	SCITEPRESS - Proceedings of DATA 2019	Proposes a four-phase (Identify, Insulate, Inspect, Improve) approach to data governance and risk management in IoT-enabled digital IS ecosystems. Demonstrates with a case study of wearable data (Fitbit)	Governance Framework	Qualitative	Conceptual Study, Single case study	Literature review	

						and the challenges of privacy, data classification, patch management, and retention policies within healthcare contexts.					
P4	RQ1	A Converged Cloud-Fog Architecture for Future eHealth Applications	(Dang et al., 2021)	Conference Paper	IEEE Xplore	This paper addresses 5G's role as an integrator for distributed computing (cloud + edge/fog) and IoT in eHealth. Identifies diverse eHealth use cases, outlines a layered architecture (device layer, multi-access edge layer, 5G network layer, multi-cloud infrastructure) and demonstrates an example with smartphone-based heart rate regression and distributed AI for patient monitoring.	Reference Architecture	Quantitative	Conceptual Study, Single case study	Case study	
P5	RQ2	A Framework for Project Risk Assessment in Telehealth	(Sulis et al., 2021)	Conference Paper	IEEE/ACM Conference on Connected Health (CHASE)	Introduces a 5-phase approach (Identification, Mapping, Evaluation, Monitoring, Mitigation) for IT risk assessment in healthcare, using a GRC platform. Illustrates the method on a multi-partner telehealth project employing HPC4AI, IoT devices, AI, and patient data. Focuses on synergy of data privacy, security, compliance, and risk management for eHealth.	Governance Framework	Qualitative	Conceptual Study, Single case study	Case study	Italy
P6	RQ2	A Governance Model for Managing Lightweight IT	(Bygstad & Iden, 2017)	Conference Paper	Springer International Publishing - AIST (Advances in Intelligent Systems and Computing)	This paper identifies four distinct governance approaches to address the growing phenomenon of lightweight IT smaller, user-driven, or third-party-developed solutions. It contrasts them with heavyweight IT's centralized, standardized approaches. The eHealth domain examples	Governance Framework	Qualitative	Conceptual Study	Literature review	Norway

						(hospital boards, local clinics) illustrate how these governance models could adapt to local innovative solutions while maintaining organizational policy and security.					
P7	RQ1	A Model-Driven Framework to Develop Personalized Health Monitoring	(Venčkauskas et al., 2016)	Journal Article	Symmetry (MDPI)	Presents a multi-layered approach to designing PHM applications that collect data from wearable sensors, handle data privacy, and manage energy constraints. Encourages "feature modeling" to systematically represent functional and non-functional aspects (security protocols, sensor energy usage) and then transform those models into actual code for a prototype. The approach merges IoT, healthcare, and model-driven engineering for flexible and personalized solutions.	Reference Architecture	Quantitative	Single case study	Case study, Experiment, Modeling, Literature review	
P8	RQ1, RQ2	A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT	(Gohar et al., 2022)	Journal Article	IEEE Access	The paper addresses the challenge of fragmented, application-centric health systems by shifting to a patient-centric approach. Presents a 5-tier architecture integrating IoT for data collection, blockchain for secure data sharing (permissioned ledger), and a transformation layer for semantic alignment of health data. Demonstrates potential to unify multiple healthcare systems, ensuring tamper-proof records, identity management, access control, and HL7-based interoperability.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study	Literature review	

P9	RQ1	A Reference Architecture for Smart Digital Platform for Personalized Prevention and Patient Management	(Elgammal & Krämer, 2021)	Book Section	Springer Nature (LNCS)	The paper presents a layered digital platform architecture integrating IoT devices, data lake structures, metadata management, and effective data governance. It emphasizes scalability, security, privacy, and interoperability to support 4P medicine (Predictive, Preventive, Personalized, Participative).	Reference Architecture	Qualitative	Conceptual Study	Literature review	
P10	RQ1	A review of edge computing reference architectures and a new global edge proposal	(Sittón-Candanedo et al., 2019)	Journal Article	Elsevier (Future Generation Computer Systems)	The paper reviews prominent edge computing reference architectures (FAR-Edge, Intel-SAP, ECC, IIC) and discusses their advantages and limitations. It then proposes a novel tiered architecture adding blockchain-based security for Industry 4.0 and other scenarios.	Reference Architecture	Mixed Method	Conceptual Study, Literature review	Literature review	
P11	RQ1	A Standard-Based and Context-Aware Architecture for Personal Healthcare Smart Gateways	(Santos et al., 2016)	Journal Article	Springer (Journal of Medical Systems)	The paper proposes an architecture for a personal healthcare gateway that recognizes when medical sensors (e.g., blood pressure or ECG) need priority network access. It uses ISO/IEEE 11073 data extraction to identify medical traffic and manage quality of service in a personal area network shared with non-medical devices.	Reference Architecture	Quantitative	Conceptual Study	Literature review	
P12	RQ1, RQ2	A Unified Smart City Model (USCM) for Smart City Conceptualization and Benchmarking	(Anthopoulos et al., 2016)	Journal Article	IGI Global (International Journal of Electronic Government Research)	The paper reviews a variety of reference architectures and frameworks for smart cities, identifies key components and dimensions (such as economy, mobility, environment, people, governance, living), and proposes a unified conceptual model plus	Governance Framework + Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review	

						guidelines for measuring city performance.					
P13	RQ1, RQ2	Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems	(Talaminos-Barroso et al., 2022)	Journal Article	Measurement: Sensors (Elsevier)	The paper highlights the lack of an IEEE 2413 extension for healthcare. It proposes how to use the standard's architectural framework and security viewpoints for IoMT solutions, describing stakeholders, concerns, and a layered architecture with an example use case of a wearable-based COPD patient monitoring system.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Literature review	
P14	RQ1	AIoTES: Setting the principles for semantic interoperable and modern IoT-enabled reference architecture for Active and Healthy Ageing ecosystems	(Valero et al., 2021)	Journal Article	Elsevier (Computer Communications)	In the ACTIVAGE project, the authors developed an IoT ecosystem suite, AIoTES, which unifies heterogeneous IoT platforms supporting AHA services. AIoTES includes a semantic interoperability layer, big data analytics, and integrated security to allow for cross-platform data sharing and application reuse across multiple deployment sites.	Reference Architecture	Quantitative	Single case study	Case study, Literature Review	Multi-country EU large scale pilot (Spain, Italy, Greece, etc.)
P15	RQ1	An architectural framework of elderly healthcare monitoring and tracking through wearable sensor technologies	(Alsadoon et al., 2024)	Journal Article	Springer (Multimedia Tools and Applications)	The paper proposes an SDD taxonomy (Sensing, Data Storage, and Data Communication) to improve the accuracy and reliability of remote elderly healthcare. It reviews wearable technologies, suggests a multi-component approach (sensors, data analysis, big data cloud) for better health monitoring and alerts.	Reference Architecture	Mixed Method	Conceptual Study, Literature review	Literature review	
P16	RQ1, RQ2	An Enhanced and Secure Cloud Infrastructure for e-Health Data Transmission	(Memos et al., 2021)	Journal Article	Springer (Wireless Personal Communications)	The paper proposes a novel 4-layer cloud model to handle the exponential growth of malware and security threats in e-health networks.	Governance Framework + Reference Architecture	Quantitative	Conceptual Study	Experiment, Literature Review	

						Emphasizes low memory usage, privacy-preserving data exchange (only partial data signatures stored in the cloud), and resource optimization via virtualization to reduce energy usage.					
P17	RQ1, RQ2	An IoT Equipped Hospital Model: A New Approach for E-governance Healthcare Framework	(Kakkar, 2019)	Journal Article	International Journal of Medical Research & Health Sciences	Highlights the importance of IoT to improve access to healthcare in rural India. Suggests a bottom-up approach: small local clinics (GCSK) at village level connect to an advanced IoT-equipped hospital at the state level. Incorporates telemedicine, smart sensors, e-records, and cloud-based data. Mentions security but not deeply elaborated.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	India
P18	RQ1, RQ2	ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC	(M. Kumar et al., 2022)	Journal Article	IEEE Transactions on Industrial Informatics	Addresses IoMT vulnerabilities by introducing a multi-step security approach: user & node authentication, privacy via EKA, data classification for sensitivity, encryption with RECC-VC, plus blockchain for data integrity. The architecture specifically aims to protect sensitive medical data while sustaining performance in IoMT networks.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study, Single case study	Case study, Experiment	
P19	RQ1, RQ2	Blockchain and LDP Based Smart Healthcare IoT Applications Architecture, Challenges and Future Work	(Iftikhar et al., 2023)	Conference Paper	IEEE Xplore	Paper highlights security vulnerabilities in typical healthcare IoT. Compares existing frameworks. Then proposes a 4-layer architecture: Medical Equipment Layer, Blockchain Layer, LDP Layer, and Cloud (Icedrive). Emphasizes encryption, local privacy, and	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Survey	

						decentralized trust to protect patient data.					
P20	RQ1, RQ2	Blockchain Based e-Healthcare Data Sharing Framework	(Borse & Sharma, 2024)	Conference Paper	IEEE (ICBDS 2024)	Discusses the state-of-the-art in e-health systems, the role of blockchain in ensuring data immutability and trust. Presents a conceptual design dividing data producers (hospitals, personal devices) and consumers (labs, insurance, eGov) with a blockchain solution for secure sharing. Mentions anonymization and access control.	Governance Framework + Reference Architecture	Quantitative	Conceptual Study, Literature review	Literature review, Survey	
P21	RQ1, RQ2	Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study	(Hasselgren et al., 2021)	Journal Article	Journal of Medical Internet Research	Points out trust issues in Healthcare 4.0 as care is virtualized. Focuses on verifying competence of providers, a crucial factor for patient trust. Presents an Ethereum-based prototype storing cryptographically hashed references to professionals' credentials and care experience. Addresses partial GDPR alignment by not storing personal data on-chain.	Governance Framework + Reference Architecture	Mixed Method	Single case study	Case study, Literature Review	Norway
P22	RQ1	Blockchain for Industry 4.0: A Comprehensive Review	(Bodkhe et al., 2020)	Journal Article	IEEE Access	Explores blockchain applicability in Industry 4.0-based applications, discusses architecture, security, privacy, and potential frameworks, and compares existing solutions.	Reference Architecture	Qualitative	Systematic literature review	Literature review	
P23	RQ1	Challenges and Solutions for Designing and Managing pHealth Ecosystems	(Blobel, 2019)	Journal Article	Frontiers in Medicine	Discusses paradigm changes toward personalized, preventive, predictive, participative precision medicine and proposes a system-oriented, architecture-centric, ontology-based, policy-driven approach for pHealth ecosystems.	Reference Architecture	Qualitative	Conceptual Study	Modeling	

P24	RQ1, RQ2	Cloud Computing Security Framework Based on Shared Responsibility Models	(U. K. Singh & Sharma, 2021)	Book Section	Taylor & Francis (CRC Press)	Presents an overview of cloud architectures, references the NIST 3–4–5 model, highlights the shared responsibility of security among CSP and end-users, and proposes a security framework for cloud environments with risk mitigation strategies.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	
P25	RQ1	Cognition Based Fog layer to Mitigate the challenges of Real-Time Medical Applications	(Kalingarani & Selvaraj, 2022)	Conference Paper	IEEE Xplore	Examines limitations of cloud-only solutions for time-critical health care data. Proposes an intermediary fog layer that integrates with edge devices to enable faster response and reliability for real-time health applications.	Reference Architecture	Quantitative	Conceptual Study	Conceptual analysis	
P26	RQ1, RQ2	Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework	(Mackey et al., 2020)	Journal Article	Journal of Medical Internet Research	Addresses the need to involve patients, providers, and payers in verifying health care claims. Describes a conceptual approach for a private/consortium blockchain with smart contracts to improve claim validation. Includes a prototype that maps the Medicare claims adjudication process onto Ethereum.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study, Single case study	Case study, Literature Review	United States
P27	RQ1, RQ2	Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors	(Khowaja et al., 2018)	Journal Article	Computer Networks (Elsevier)	Presents an architecture called HIoTSP that collects data from wearable devices (inertial, physiological, location sensors), processes them in a middleware (smartphone) and server for activity recognition, and automatically selects relevant healthcare services. Demonstrates system's feasibility by implementing fall and stress detection, showing real-time alerts and visualizations.	Governance Framework + Reference Architecture	Quantitative	Conceptual Study, Single case study	Case study, Experiment	

P28	RQ1, RQ2	Control Systems Cyber Security Reference Architecture (RA) for Critical Infrastructure: Healthcare and Hospital Vertical Example	(Scalco et al., 2021)	Journal Article	Journal of Critical Infrastructure Policy	This paper extends the DoD CIO Cyber Security Reference Architecture (CSRA) with an appendix for control systems. They adapt it to a healthcare/hospital environment, describing the threats (ransomware, malware) and possible solutions (network segmentation, zero trust). They highlight a pilot demonstration in the energy sector and draw parallels for healthcare. The RA aims to guide governance, risk-based decisions, and future policy for hospital networks.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study	
P29	RQ1, RQ2	COUNT: Blockchain framework for resource accountability in e-healthcare	Kumar et al., 2023	Journal Article	Computer Communications (Elsevier)	This paper addresses medical supply management, balancing demand/supply of hospital resources. Proposes a consortium blockchain called COUNT that records resource requests, availability, and usage, ensuring accountability among healthcare stakeholders (patients, hospitals, suppliers). The novel COUNT-PoV consensus involves multi-stakeholder voting for blocks. Also uses a signcryption approach to reduce cryptographic overhead.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study	Simulation	
P30	RQ1, RQ2	Decentralized Privacy-Preserving Framework for Health Care Record-Keeping Over Hyperledger Fabric	(B. Prasad & Ramachandram, 2021)	Book Section	Springer	This work explores the use of private blockchain (Hyperledger Fabric) to store and share EHR data among different healthcare stakeholders. Emphasizes user anonymity via group signatures, so the blockchain validator can confirm	Governance Framework + Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study	

						authenticity without revealing user identity. Aims to ensure EHR confidentiality, data integrity, and restricted access, referencing standard HPC rules (HIPAA, partially).					
P31	RQ1	Developing an Architecture for IoT Interoperability in Healthcare: A Case Study of Real-time SpO2 Signal Monitoring and Analysis	(Nguyen et al., 2020)	Conference Paper	IEEE Big Data Conference Proceedings	Presents a novel IoT reference architecture that includes gateways and data converters to address interoperability challenges for healthcare IoT. Uses open-source analytic platforms for real-time SpO2 monitoring/analysis. Demonstrates feasibility using a small-scale case study/laboratory setting.	Reference Architecture	Mixed Method	Conceptual Study, Single case study	Case study	
P32	RQ1	Digital Twin Perspective of Fourth Industrial and Healthcare Revolution	(Khan et al., 2022)	Journal Article	IEEE Access	Surveys how digital twin (DT) has emerged as a key enabler for Industry 4.0 and Healthcare 4.0, detailing reference architectures (RAMI 4.0) and discussing different layers (IoT, edge, AI, big data) needed to form end-to-end digital twin solutions. Covers potential benefits in healthcare (e.g., real-time patient data modeling) and open issues (security, standards).	Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review, Modeling, Survey	
P33	RQ1	Disruptive Technologies for Environment and Health Research: An Overview of Artificial Intelligence, Blockchain, and Internet of Things	(M. Bublitz et al., 2019)	Journal Article	International Journal of Environmental Research and Public Health	This paper explores the current uses of disruptive technologies (AI, blockchain, IoT) in environment and health, discussing potential applications, challenges, and a conceptual architecture for a pan-Canadian monitoring and surveillance system. Highlights the synergy of these technologies for analyzing large datasets and protecting data integrity in	Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	Canada

						environmental and healthcare contexts.					
P34	RQ1	DT-IoMT: A Digital Twin Reference Model for Secure Internet of Medical Things	(Kabir & Ray, 2024)	Conference Paper	IEEE Xplore	Focuses on the synergy of digital twin concepts with IoMT in healthcare. Introduces a reference architecture that merges physical twins (patient, medical devices) with virtual twins (data modeling, real-time states) for advanced monitoring, security, and predictive analysis in chronic disease management. Emphasizes the importance of robust cybersecurity while introducing a conceptual layered design for integrating real-time data from medical sensors.	Reference Architecture	Qualitative	Conceptual Study	Modeling, Literature Review	
P35	RQ1, RQ2	EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange	(Akkaoui et al., 2020)	Journal Article	IEEE Access	Presents EdgeMediChain, a parallelized architecture employing local edge-mining pools plus a global blockchain for efficient, scalable, and privacy-preserving health data exchange. Demonstrates how edge computing nodes can handle large IoT data volumes, offloading network traffic, while blockchain (Ethereum-based) enforces secure authentication, authorization, and tamper-proof data logs.	Governance Framework + Reference Architecture	Quantitative	Conceptual Study, Single case study	Case study, Literature Review	
P36	RQ1	Enabling pandemic-resilient healthcare: Narrowband Internet of Things and edge intelligence for real-time monitoring	(Islam et al., 2023)	Journal Article	Wiley Online Library / CAAI Transactions on Intelligence Technology (John Wiley & Sons, IET)	The paper introduces a novel NB-IoT-based framework to connect smart monitoring devices in healthcare facilities, ensuring data security, performance, and reduced reliance on central data centers. It highlights how edge computing can improve	Reference Architecture	Qualitative	Conceptual Study	Literature review	

						coverage, reduce power consumption, and handle real-time data processing in pandemic scenarios.					
P37	RQ2	Enhancing Transparency and Trustworthiness of Healthcare IoT Data with AWS: A Proposed Model	(Ali et al., 2024)	Conference Paper	Springer (LNICST series)	Proposes a comprehensive framework leveraging AWS services (S3, KMS, IAM, CloudTrail, Redshift, etc.) to ensure secure data storage, encryption, access controls, and anonymization techniques, thereby strengthening transparency and trust in healthcare IoT data.	Governance Framework	Qualitative	Conceptual Study, Single case study	Case study, Literature review	
P38	RQ2	Ethical Considerations in the Integration of Internet of Things (IoT) Technologies Within Digital Health: A Comprehensive Framework for Evaluation	(Wakili & Bakkali, 2024)	Conference Paper	Springer (LNNS series)	The paper presents a multi-dimensional framework to systematically assess ethical implications of IoT technologies in digital health. Key dimensions include data privacy, informed consent, algorithmic fairness, transparency, and regulatory compliance.	Governance Framework	Mixed Method	Literature review	Interviews	
P39	RQ2	Exploring the Scope of Policy Issues Influencing IoT Health and Big Data: A Structured Review	(Maina & Singh, 2022)	Book Section	Published in 'Global Healthcare Disasters' (CRC Press or similar)	A structured review identifying eight main policy themes hindering or driving big data/IoT integration in healthcare, including data sharing, privacy, security, standards, stakeholders, human capital, funding, and legal/regulatory matters. Recommends guidelines for improved data governance and updated consent protocols.	Governance Framework	Qualitative	Literature review	Literature review	
P40	RQ1	Federated Learning for the Internet-of-Medical-Things: A Survey	(V. K. Prasad et al., 2023)	Journal Article	MDPI (Mathematics 2023, 11, 151)	The survey categorizes FL approaches (CFL, DFL), outlines a reference FL-IoMT architecture, discusses security challenges and trust solutions, and proposes a	Reference Architecture	Qualitative	Conceptual Study	Case study, Survey	

						blockchain-based FL scheme (Cross-FL) with performance analysis. It covers open issues and potential future research directions in FL for IoMT healthcare applications.					
P41	RQ1	Fog-centric IoT Smart Healthcare: Architecture, Applications, and Case Study	(Gupta et al., 2024)	Journal Article	Springer (LN in Networks and Systems)	Presents a three-layer fog-based healthcare IoT architecture. Describes device layer (sensors, wearables), fog layer (gateways, local servers), and cloud layer. Demonstrates advantages in reducing latency, local data processing, and real-time services. Showcases a wearable (smart gloves) case study for patient monitoring.	Reference Architecture	Qualitative	Conceptual Study, Single case study	Case studies	
P42	RQ1	Fusion of IoT, AI, Edge–Fog–Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine	(Firouzi et al., 2023)	Journal Article	IEEE Xplore	Analyzes the technological interplay (IoT, AI, blockchain, edge–fog–cloud) in various domains, focusing on healthcare. Details how each technology addresses limitations of the others, proposes a conceptual architecture, and illustrates via a stress monitoring case study. Emphasizes improved data privacy, low latency, interoperability, and risk management.	Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study	
P43	RQ1	Health Monitoring & Management using IoT devices in a Cloud Based Framework	(Sharma et al., 2018)	Conference Paper	IEEE Xplore	Introduces an IoT ecosystem for remote health monitoring using sensors for body temperature, heart rate, ECG, accelerometer, etc. Data is streamed to a cloud for analysis. Proposes a 'health index' concept to interpret multiple sensor readings. Emphasizes user-friendly, real-time solution, though	Reference Architecture	Mixed Method	Conceptual Study, Single case study	Case study	

						security and standardization are only briefly touched upon.					
P44	RQ1	Imtidad: A Reference Architecture and a Case Study on Developing Distributed AI Services for Skin Disease Diagnosis over Cloud, Fog and Edge	(Janbi et al., 2022)	Journal Article	Sensors (MDPI)	Describes the Imtidad framework for building/distributing AI-based healthcare services at scale. Illustrates usage with deep learning models (standard + Tiny AI versions) for dermatology diagnosis, tested on multiple hardware (cloud VMs, Jetson Nano, Pi, smartphones) and networks, analyzing latency, energy, and feasibility of real-time usage.	Reference Architecture	Quantitative	Single case study	Case study	
P45	RQ1	Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation	(Aguru et al., 2022)	Journal Article	MDPI (Algorithms)	Presents a comprehensive investigation of common IoT architectures (ETSI, ITU-T, IoT-A, Intel, etc.) and addresses IoT challenges in healthcare. Proposes a novel SHRA built on the IoT World Forum's 7-layer approach for hospital and medical service optimization, with coverage of data processing, connectivity, security, and governance.	Reference Architecture	Qualitative	Systematic literature review	Literature review	
P46	RQ1	Integration of Cloud and IoT for smart e-healthcare	(Shah et al., 2021)	Book Section	Elsevier (in 'Healthcare Paradigms in the Internet of Things Ecosystem')	Covers how combining cloud computing with IoT can enhance remote healthcare services. Outlines a conceptual architecture for IoT-based health data collection and cloud-based analytics. Explores security challenges and open research areas for large-scale e-health. Presents use cases for remote patient monitoring, telemedicine, resource optimization.	Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review, Survey	
P47	RQ1	Internet of medical things and blockchain-enabled	(Rahman et al., 2024)	Journal Article	Nature Scientific Reports	Describes a system for e-health with integrated IoMT devices, leveraging a patient-	Reference Architecture	Mixed Method	Conceptual Study	Prototype	

		patient-centric agent through SDN for remote patient monitoring in 5G network				centric agent to handle data ownership in a 5G environment. Uses blockchain to protect patient data, SDN to control flows, and ensures privacy. Demonstrates efficiency and security improvements via prototype on Hyperledger Fabric with HPC-like methods, analyzing throughput, overhead, and reliability.					
P48	RQ1	Internet of Things Based Context Awareness Architectural Framework for HMIS	(Pir et al., 2015)	Conference Paper	IEEE Xplore (IEEE Healthcom Workshop)	Describes the use of context awareness in an IoT architecture to reduce data overload from massive sensor deployments in hospitals. Architecture includes a middleware layer that captures relevant data, merges it with contextual info, and ensures only required data is forwarded. Aims to improve IoT-based HMIS functionality and minimize big data complexity.	Reference Architecture	Qualitative	Conceptual Study, Single case study	Simulation	
P49	RQ1	IOE Solution for A Diabetic Patient Monitoring	(Ismail, 2017)	Conference Paper	IEEE Xplore (International Conference on Information Technology - ICIT)	Introduces a healthcare IoE architecture specifically for type 1 diabetes management. The system uses an implanted glucose meter and a health monitoring company to proactively react to abnormal glucose levels. Distinguishes between proactive and reactive data transmissions. Uses cloud for storing data and notifies patient or dispatches help in critical states.	Reference Architecture	Quantitative	Conceptual Study, Single case study	Simulation	
P50	RQ1, RQ2	IoT Enabled Elderly Monitoring System and the Role of Privacy Preservation	(Aski et al., 2022)	Conference Paper	Springer (Lecture Notes on Data Engineering and	Presents an IoT-based architecture for remotely monitoring elderly or differently abled patients,	Governance Framework + Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review	

		Frameworks in e-health Applications			Communications Technologies)	highlighting privacy protection frameworks and the associated security challenges. Discusses the role of WSN/WSN technology, advanced connectivity, data flow naming, and access controls for privacy.					
P51	RQ1, RQ2	IoT-Gov: A structured framework for internet of things governance	(Sedrati et al., 2023)	Journal Article	Elsevier (Computer Networks, Vol 233)	The paper develops IoT-Gov, a multi-layer governance framework covering governance processes (identify needs, define model, implement, evaluate) and a reference architecture. It addresses challenges of roles/responsibilities, data management, standards, and security. A use-case scenario of a smart hospital parking with blockchain-based access control is presented.	Governance Framework + Reference Architecture	Mixed Method	Conceptual Study, Single case study	Literature review, Systematic literature review	
P52	RQ1	Leveraging IoT-Aware Technologies and AI Techniques for Real-Time Critical Healthcare Applications	(Shumba et al., 2022)	Journal Article	MDPI (Sensors, Vol 22)	Surveys IoT-based healthcare architectures (both centralized, decentralized). Highlights the need for real-time analysis with on-device AI, Edge Intelligence, and advanced flexible sensors. Proposes a multi-layer reference architecture with wearable sensors, local processing, edge computing, and cloud integration for timely intervention in critical health scenarios.	Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review	
P53	RQ1	Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring systems	(Sawand et al., 2014)	Conference Paper	IEEE (Symposium on Privacy and Security in CommuTations, ICCC 2014)	Highlights a patient-centric, sensor-based eHealth architecture integrating wireless body area networks (WBANs), IoT, and cloud resources. Explores energy efficiency, privacy, data authenticity, multi-device	Reference Architecture	Qualitative	Conceptual Study	Literature review	

						coordination, and crowd sensing for disease control. Underscores the tension between performance and privacy/security goals in eHealth monitoring.					
P54	RQ1	One IoT: an IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible	(Banda et al., 2016)	Journal Article	Springer (Journal of Reliable Intelligent Environments)	Describes a lightweight IoT protocol (One IoT) that outlines essential criteria for an IoT-enabled device to achieve forward compatibility. The protocol has methods for device discovery, registration, advertisement of capabilities, invocation, and configuration. Security aspects such as device keys, minimal encryption, and cloud-based mapping are addressed. Encourages OEMs to use a uniform specification so that user interfaces and device operations can be generated dynamically and remain future-proof.	Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	
P55	RQ1, RQ2	Overcoming Challenges for Improved Patient-Centric Care: A Scoping Review of Platform Ecosystems in Healthcare	(Chibuike et al., 2024)	Journal Article	IEEE Access	Surveys relevant literature on digital platforms in healthcare, discussing how multi-actor value co-creation is hindered by data security, privacy, and regulation issues. Categorizes existing solutions by domain, challenges, and solutions. Develops a conceptual ecosystem framework supporting patient-centric services and standardization attempts.	Governance Framework + Reference Architecture	Qualitative	Literature review	Literature review, Survey	
P56	RQ2	Privacy and Security Issues for IoT and Deep Learning in Next-Generation Healthcare	(Agrawal et al., 2024)	Book Section	CRC Press, from 'Deep Learning in IoT for Next Gen Healthcare' (anticipated)	Discusses the Indian healthcare landscape, role of IoT and deep learning for disease monitoring, identifies typical risks (unauthorized	Governance Framework	Qualitative	Literature review	Literature review	India

						access, data breaches, re-identification) and emerging solutions (encryption, risk assessments, compliance with HIPAA, GDPR). Recommends a multi-layer approach with robust governance, stakeholder collaboration, and technology best practices.					
P57	RQ1	Reference Architectures, Platforms, and Pilots for European Smart and Healthy Living—Analysis and Comparison	(Grguric et al., 2021)	Journal Article	Electronics (MDPI)	Presents a multi-project analysis of large eHealth/AAL pilot initiatives, extracting common patterns and gaps in architecture definitions. Applies taxonomies from existing healthcare IoT references, picks CREATE-IoT 3D RAM as recommended standard. Observes that many solutions revolve around communication support, reminders, monitoring, guidance for older adults. Emphasizes interoperability, security, data exchange as cross-cutting concerns.	Reference Architecture	Qualitative	Literature review	Literature review, Survey	European Union
P58	RQ1	Research on the Fusion Model Reference Architecture of Sensed Information of Human Body for Medical and Healthcare IoT	(He et al., 2018)	Conference Paper	Proceedings of the 17th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)	Building on the IoT six-domain model, authors define a reference architecture capturing how multi-source data from sensors is fused across five levels (preprocessing, object estimation, population state, impact estimation, and optimized control). They illustrate the architecture's functional domains (user, sensing control, service providing, operation mgmt, resource exchange, target domain). They test the	Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study, Modeling	

						approach with a sleep monitoring scenario, highlighting data flows from sensors to aggregated analysis.					
P59	RQ1, RQ2	Scalable and Security Framework to Secure and Maintain Healthcare Data using Blockchain Technology	(Mahammad & Kumar, 2023)	Conference Paper	IEEE Xplore	Argues that integrating blockchain with big data solutions can offer secure, scalable storage of healthcare data (EHR). Emphasizes trustless data exchange, cryptographic proofs, consensus, and replication for resilience. Proposes an architecture that harnesses big data technologies (e.g., Hadoop/HDFS, NoSQL) alongside blockchain layers to ensure data integrity, high capacity, and privacy for EHR management.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Prototype	
P60	RQ1	SDN_Based Secure Healthcare Monitoring System (SDN-SHMS)	(Khayat et al., 2019)	Conference Paper	IEEE Xplore	Examines vulnerabilities in typical healthcare monitoring systems that rely on IoT devices. Integrates SDN as the core communication and control layer, enabling flexible and centralized management of security policies. Proposes a multi-layer architecture including sensors, mobile apps, an SDN controller, and a security platform with modules for intrusion detection, prevention, authentication, and access control.	Reference Architecture	Qualitative	Conceptual Study	N/A	
P61	RQ1	Securing 5G-Enabled Internet of Medical Things in Healthcare: Vulnerabilities, Threats, and	(Preetham et al., 2023)	Conference Paper	IEEE Xplore	Highlights how IoMT can enhance remote patient management using 5G's high bandwidth and low latency, but faces numerous security vulnerabilities including DoS, DDoS, advanced persistent	Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	

		Architectural Framework				threats, data tampering, and privacy breaches. Proposes a layered approach (device, network, cloud/edge, application) with encryption, authentication, SDN-based management, and intrusion detection. Aims to guarantee patient data confidentiality, system integrity, and availability for real-time e-health scenarios.					
P62	RQ1, RQ2	Securing Mobile e-Health Environments by Design: A Holistic Architectural Approach	(Aranha et al., 2019)	Conference Paper	IEEE e-Health Workshop	Healthcare is recognized as a critical sector requiring advanced security. Many e-health solutions rely on modular architecture, but typically lack a consolidated approach that merges interoperability and robust security, especially for mobile devices. Authors combine the IHE's reference approach, RAMI 4.0 (from Industry 4.0) for layered architecture, and the RMIAS security model to systematically identify, classify, and address security requirements from design-time through device lifecycle. Illustrates the approach with a use case of mobile medical devices exchanging data with a hospital via the IHE MHD standard.	Governance Framework + Reference Architecture	Qualitative	Conceptual Study	Conceptual analysis	
P63	RQ1	Security Implications in the Transformation of Healthcare Through Internet of Things Devices	(George Ray et al., 2021)	Journal Article	Issues in Information Systems (IIS)	Presents a four-part IoT architecture for medical solutions: devices, gateways, applications, platform. For each part, the authors systematically identify vulnerabilities (malicious code insertion, eavesdropping, insecure gateway comm, etc.).	Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review	

						Recommends standard security measures: encryption in transit, strong authentication, code signing, intrusion detection, etc. Argues that a holistic approach from sensor to platform is essential in e-health, especially in African markets where 'ASSURED' medical devices are increasingly popular.					
P64	RQ1	Smart healthcare IoT applications based on fog computing: architecture, applications and challenges	(Quy et al., 2022)	Journal Article	Complex & Intelligent Systems (Springer), Vol. 8	Compares cloud, edge, and fog paradigms, then presents a general fog-based architecture for IoT healthcare scenarios. Illustrates use cases (e.g., continuous patient monitoring, emergency response) and identifies open challenges and future directions for robust, low-latency healthcare IoT solutions.	Reference Architecture	Qualitative	Conceptual Study, Literature review	Literature review	
P65	RQ1	Software architecture for IoT-based health-care systems with cloud/fog service model	(Hajvali et al., 2022)	Journal Article	Springer (Cluster Computing 2022, 25:91–118)	Presents a multi-layer reference architecture with IoT device layer, fog sub-layers, and a cloud layer. Uses UML 4+1 views and graph transformations for formal modeling, verifying system reliability and performance. Demonstrates a user mobility scenario and uses ATAM for architectural trade-off analysis.	Reference Architecture	Quantitative	Conceptual Study	Modeling	
P66	RQ1	Survey Based Analysis of Internet of Things Based Architectural Framework for Hospital Management System	(Muhammad et al., 2015)	Conference Paper	IEEE Xplore (13th Intl Conf on Frontiers of Information Technology)	Examines limitations of existing HMIS in Pakistan, proposes an architectural approach integrating IoT sensors and context-awareness to improve monitoring, communication, early diagnosis. Includes a	Reference Architecture	Qualitative	Conceptual Study	Survey	Pakistan

						questionnaire-based survey among healthcare staff, indicating positive acceptance of IoT-based HMIS approach.					
P67	RQ1, RQ2	The architectural divergence problem in security and privacy of eHealth IoT product lines	(Tomashchuk et al., 2021)	Conference Paper	ACM (SPLC '21, Leicester, UK)	Describes the HEART eHealth IoT platform as a product line with a reference architecture and multiple variants. Uses STRIDE and LINDDUN (implemented via SPARTA) for threat modeling. Observes that small changes in data or processes drastically alter threat surfaces, calling this the "architectural divergence problem."	Governance Framework + Reference Architecture	Qualitative	Single case study	Case study, Modeling	
P68	RQ1	The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT)	(Firouzi et al., 2022)	Journal Article	Elsevier (Information Systems, Volume 107)	This paper discusses the synergy among cloud, fog, and edge computing for IoT, highlighting how each layer addresses scalability, latency, and data processing. It proposes a hierarchical reference model (edge–fog–cloud) and examines key design aspects (resource allocation, offloading, security, etc.) for AI-enabled IoT.	Reference Architecture	Qualitative	Conceptual Study	Literature review	
P69	RQ1	The Convergence of Cloud, IoT, and Artificial Intelligence for Intelligent Systems	(K. D. Singh et al., 2024)	Book Section	CRC Press	Provides an overview of the synergy among cloud, IoT, and AI that drives data analytics, automation, and novel applications. Discusses building blocks of intelligent systems, including data acquisition, preprocessing, model training, and security/privacy considerations.	Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study	
P70	RQ1	The convergence of IoT and distributed ledger technologies	(Farahani et al., 2021)	Journal Article	Elsevier (Journal of Network and Computer	Surveys DLT fundamentals, including blockchain and DAG solutions, and outlines	Reference Architecture	Qualitative	Conceptual Study	Literature review	

		(DLT): Opportunities, challenges, and solutions			Applications, Volume 177)	how these can fix security and trust gaps in IoT. Proposes a holistic reference architecture for blockchain-IoT in healthcare, discussing open issues such as scalability, privacy, consensus algorithms, and standardization.					
P71	RQ1	The IoT Architectural Framework, Design Issues and Application Domains	(Gardašević et al., 2017)	Journal Article	Springer (Wireless Personal Communications)	Provides an overview of reference IoT layers (6LoWPAN, ZigBee, CoAP, MQTT), addresses hardware constraints and OS choices, and discusses case applications, including healthcare. Presents preliminary performance results for protocols like MQTT and TSCH tested on OpenMote with Contiki/OpenWSN.	Reference Architecture	Quantitative	Single case study	Case study	
P72	RQ1	The monitoring and managing application of cloud computing based on Internet of Things	(Luo & Ren, 2016)	Journal Article	Computer Methods and Programs in Biomedicine (Elsevier)	Presents a comprehensive model (RMCPHI) that integrates body sensors, home gateways, and cloud servers for real-time healthcare data collection and analysis. Emphasizes how cloud computing and IoT can improve patient monitoring (e.g., for chronic diseases, vital signs) and offer cost-effective solutions. Proposes an efficient PSOSAA algorithm to optimize resource usage and scheduling for data processing in a medical context.	Reference Architecture	Mixed Method	Conceptual Study, Single case study	Simulation	
P73	RQ2	'The plural of silo is not ecosystem': Qualitative study on the role of innovation	(Reidy et al., 2023)	Journal Article	SAGE Publications (Digital Health)	Uses the NASSS framework to study IoT-based solutions, focusing on heart monitoring and assistive technologies in a region in South East England.	N/A	Qualitative	Conceptual Study	Semi-structured interviews	UK

		ecosystems in supporting 'Internet of Things' applications in health and care				Interviewees share experiences about system fragmentation, limited resources, procurement and policy misalignment. Argues the need for multi-stakeholder collaboration, strategic alignment of interests, and integrated data pathways to achieve real-world IoT impact.					
P74	RQ1	Toward energy-efficient and trustworthy eHealth monitoring system	(Sawand et al., 2015)	Conference Paper	China Communications (IEEE), Conference Proceeding	Presents a holistic framework for eHealth, focusing on data collection via wearable sensors, crowd sensing, and cloud data processing. Examines performance goals (energy, reliability) vs. security (privacy, confidentiality). Reviews security threats, discusses trust, privacy by design, risk management, and outlines open design challenges (i.e., tradeoff between security overhead and sensor constraints).	Reference Architecture	Qualitative	Conceptual Study, Single case study	Case study, Survey	
P75	RQ1	Trends, Technologies, and Key Challenges in Smart and Connected Healthcare	(Navaz et al., 2021)	Journal Article	IEEE Access	Reviews the broad landscape of technology drivers (IoT, AI, blockchain, robotics) shaping SCH solutions for chronic disease management, remote monitoring, and telehealth. Introduces a layered reference model capturing data layers, connectivity, cloud/fog, analytics, and user interfaces. Shows how these technologies have been applied in COVID-19 scenarios for disease detection, tracing, resource allocation. Summarizes challenges: data security,	Reference Architecture	Qualitative	Literature review	Literature review	

						interoperability, standardization, user acceptance, and policy gaps.					
P76	RQ1, RQ2	Zeus: IoT-based Healthcare Data Management Security Framework for Remote Patient Monitoring	(Nuguri et al., 2023)	Conference Paper	ACM HealthSec	Introduces a reference architecture that integrates IoT sensors, edge gateways, and cloud for real-time patient data collection, storage, and analytics. Incorporates NIST-based risk assessment, role-based access control, pseudonymization for privacy, and evaluation of system scalability under multiple concurrent data streams. Emphasizes a life-cycle approach to security, from data collection to storage, with minimal residual risk for HIPAA compliance.	Governance Framework + Reference Architecture	Quantitative	Single case study	Case study	

APPENDIX B

INTERVIEW QUESTIONS (ENGLISH)

No	Question
Q1	How many years of experience do you have in IoT projects for the healthcare sector?
Q2	In the healthcare sector or in the company that develops IoT applications, which position do you currently hold?
Q3	What types of IoT projects does your company or hospital carry out in the healthcare sector? Could you briefly explain?
Q4	When providing or using IoT solutions for healthcare institutions, what are the main challenges you encounter regarding human factors, project management, security, technical implementation, and operational continuity of the systems?
Q4.1	Which of these challenges affects project success the most, and why?
Q5	How do the challenges you mentioned influence the design, implementation processes, and deployment of projects?
Q6	How do these challenges impact legal compliance, security, business processes, and daily operations in the hospitals you work with or in your hospital?
Q7	Do the hospitals you serve or your own hospital, use an IT governance framework such as ISO 27001, COBIT, or another framework for IoT risk management, or do you recommend they use one? Which frameworks do you prefer and why?
Q7.1	Are there challenges you face when implementing these governance frameworks? If so, what are they?
Q8	Overall, do you believe existing IT governance models such as ISO 27001 or COBIT are sufficient for managing IoT risks in the healthcare sector? Why?
Q9	What shortcomings or limitations do you think existing governance models have in managing IoT-specific risks in the healthcare sector?
Q10	What new governance mechanisms or tools do you consider necessary to enhance the security, legal compliance, and overall management of IoT systems in the healthcare sector? Please assess this from a GRC (Governance, Risk, and Compliance) perspective.
Q10.1	How might these mechanisms or tools make project processes easier?
Q11	What elements should a newly developed IoT governance framework include to facilitate collaboration between technology providers and hospitals and to accelerate implementation processes?
Q12	When you evaluate the projects you implement in the healthcare sector through the lenses of people, process, and product, how do you assess current IoT governance approaches?
Q12.1	Within those three dimensions, which area should be prioritized for improvement and why? What steps should hospitals or technology providers take?

APPENDIX C

INTERVIEW QUESTIONS (TURKISH)

Question No	Question
Q1	Sağlık sektörüne yönelik IoT projelerinde kaç yıllık deneyime sahipsiniz?
Q2	Sağlık sektöründe ya da IoT uygulamaları geliştiren şirketinizde hangi pozisyonda çalışıyorsunuz
Q3	Çalıştığınız şirket/hastane sağlık sektöründe hangi tür IoT projeleri yürütmektedir? Kısaca açıklayabilir misiniz?
Q4	Sağlık kuruluşlarına IoT çözümleri sunarken ya da kullanırken; insan faktörleri, proje yönetimi, güvenlik, teknik uygulama ve sistemlerin operasyonel sürekliliği açısından karşılaştığınız temel zorluklar nelerdir?
Q4.1	Bu zorluklardan hangisi proje başarısını en fazla etkiliyor ve neden?
Q5	Bahsettiğiniz bu zorluklar, projelerin tasarımını, uygulama süreçlerini ve hayata geçirilmesini nasıl etkiliyor?
Q6	Söz ettiğiniz bu zorluklar, birlikte çalıştığınız hastanelerde/hastanenizde yasal uyumluluk, güvenlik, iş süreçleri ve günlük operasyonları nasıl etkiliyor?
Q7	Çözüm sunduğunuz hastaneler/hastaneniz IoT riskleri yönetimi için ISO 27001, COBIT veya başka bir IT yönetişim çerçevesi kullanıyor mu ya da hastanelere kullanmalarını öneriyor musunuz? Hangilerini tercih ediyorsunuz ve neden?
Q7.1	Bu yönetişim çerçevelerinin uygulamasında karşılaştığınız zorluklar var mı? Varsa bunlar nelerdir?
Q8	Genel olarak, ISO 27001, COBIT gibi mevcut IT yönetişim modellerinin sağlık sektöründeki IoT risklerini yönetmekte yeterli olduğunu düşünüyor musunuz? Neden?
Q9	Mevcut yönetişim modellerinin sağlık sektöründeki IoT'ye özgü riskleri yönetme konusunda hangi eksikliklere veya sınırlılıklara sahip olduğunu düşünüyorsunuz?
Q10	Sağlık sektöründeki IoT sistemlerinin güvenliği, yasal uyumluluğu ve genel yönetim süreçlerini geliştirmek için hangi yeni yönetişim mekanizmaları veya araçlarının gerekli olduğunu düşünüyorsunuz? Özellikle GRC (Yönetişim, Risk ve Uyumluluk) perspektifinden değerlendirir misiniz?
Q10.1	Bu mekanizma veya araçlar proje süreçlerini nasıl kolaylaştırabilir?
Q11	Yeni geliştirilecek bir IoT yönetişim çerçevesinin, teknoloji sağlayıcıları ile hastaneler arasındaki iş birliğini kolaylaştırması ve uygulama süreçlerini hızlandırması için hangi unsurları içermesi gerektiğini düşünüyorsunuz?
Q12	Sağlık sektöründe uyguladığınız projeleri "insan, süreç ve ürün" boyutlarıyla düşündüğünüzde, mevcut IoT yönetişim yaklaşımlarını nasıl değerlendirirsiniz?
Q12.1	Bu üç boyut içinde öncelikli olarak iyileştirilmesi gereken alan hangisidir ve neden? Bu konuda hastaneler veya teknoloji sağlayıcıları ne tür adımlar atmalıdır?

APPENDIX D

ETHICS COMMITTEE APPROVAL

T.C.
BOĞAZİÇİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler İnsan Araştırmaları Etik Kurulu (Sbinarek)

2025 AİLE YILI

Sayı : E-84391427-050.04-224622 13.03.2025
Konu : 2025-22T Kayıt Numaralı Başvurunuz Hakkında

Sayın Prof. Dr. Bilgin METİN

Tez danışmanlığını yürüttüğünüz öğrenciniz Berk Coşardemir'in "Key Challenges of Healthcare IoT Governance" başlıklı projesi ile Boğaziçi Üniversitesi Sosyal ve Beşeri Bilimler İnsan Araştırmaları Etik Kurulu (SBİNAREK)'e yaptığınız 2025-22T kayıt numaralı başvuru 17.02.2025 tarih ve 2025/02 sayılı kurul toplantısında incelenmiş ve projeye etik onay verilmesi uygun bulunmuştur.

Bu karar tüm üyelerin toplantıya on-line olarak katılımıyla ve oybirliği ile alınmıştır. Onay mektubu tüm üyeler adına Komisyon Başkanı tarafından e-imzalanmıştır. Bilgilerinizi rica ederiz.

Saygılarımızla,

Dr. Öğr. Üyesi Işıl ERDUYAN
Kurul Başkanı

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Kodu : 090H-M68J-00G0 Belge Doğrulama Adresi : https://www.turkiye.gov.tr/bogazici-universitesi-ebys

Adres: Boğaziçi Üniversitesi 34342 Bebek/ İstanbul
Telefon No: Faks No:
e-Posta: İnternet Adresi: www.bogazici.edu.tr
Kep Adresi: bogaziciuniversitesi@hs01.kep.tr

Bilgi İçin: Nurşen MUNAR
Mühendis
Telefon No: 0 212 359-6749

APPENDIX E

GOVERNANCE FRAMEWORKS CHALLENGE COVERAGE

Study ID	Security and Privacy	Data Management	Interoperability-Standards	Scalability	Regulatory Compliance	Accountability and Transparency	Latency/Real-Time Performance	Device Management	Mobility	Energy Efficiency	Ethical Concerns	Patient Acceptance and Awareness	User Resistance and Adoption Barriers
P2	1	1	0	1	0	1	1	0	1	0	1	1	0
P3	1	1	0	0	1	1	0	0	0	0	1	1	0
P5	1	1	0	0	1	1	0	0	0	0	0	0	0
P6	1	0	1	0	0	1	0	0	0	0	0	0	0
P8	1	1	1	1	0	0	0	0	0	0	0	0	0
P12	0	0	1	1	0	1	0	0	0	0	0	0	0
P13	1	0	1	0	0	1	0	0	0	0	0	0	0
P16	1	1	0	1	0	0	1	0	0	0	0	0	0
P17	1	1	0	0	1	1	0	0	0	0	0	0	0
P18	1	1	1	1	0	0	1	0	0	0	0	0	0
P19	1	1	1	0	0	1	0	0	0	0	0	0	0
P20	1	1	0	1	0	1	0	0	0	0	0	0	0
P21	1	1	0	0	0	1	0	0	0	0	0	1	0
P24	1	1	0	1	0	1	0	0	0	0	0	0	0
P26	1	0	0	0	1	1	0	0	0	0	0	0	0
P27	0	1	1	1	0	0	1	0	0	1	0	0	0
P28	1	0	1	0	1	1	0	1	0	0	0	0	0
P29	1	1	0	1	1	1	0	0	0	0	0	0	0
P30	1	1	0	0	1	0	0	0	0	0	0	0	0

P35	1	1	0	1	1	1	1	1	1	1	0	1	0
P37	1	1	0	0	1	1	0	0	0	0	0	0	0
P38	1	0	0	0	1	0	0	0	0	0	1	1	0
P39	0	1	1	0	1	1	0	0	0	0	1	0	0
P50	1	0	1	0	0	0	0	0	0	0	0	0	0
P51	1	1	1	1	1	1	0	1	0	0	1	1	0
P55	1	1	1	1	1	0	1	0	0	0	1	0	1
P56	1	0	0	0	1	1	0	0	0	0	0	0	0
P59	1	1	0	1	1	0	0	0	0	0	0	0	0
P62	1	1	1	0	1	1	1	1	1	0	0	0	1
P67	1	1	0	0	0	0	0	0	0	0	0	0	0
P73	1	1	1	0	1	0	0	0	0	0	1	1	0
P76	1	1	1	1	1	1	0	0	0	0	0	0	0

REFERENCES

Agrawal, H. K., Agrawal, N. K., & Agrawal, S. (2024). Privacy and security issues for IoT and deep learning in next-generation healthcare: An Indian perspective. In *Deep learning in Internet of Things for next generation healthcare* (pp. 194–207). CRC Press; Scopus. https://doi.org/10.1201/9781003451846-16

Aguru, A. D., Babu, E. S., Nayak, S. R., Sethy, A., & Verma, A. (2022). Integrated industrial reference architecture for smart healthcare in Internet of Things: A systematic investigation. *Algorithms*, *15*(9), 309. https://doi.org/10.3390/a15090309

Akkaoui, R., Hei, X., & Cheng, W. (2020). EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access*, *8*, 113467–113486. https://doi.org/10.1109/ACCESS.2020.3003575

Al Shorman, O., Al Shorman, B., Al-Khassaweneh, M., & Alkahtani, F. (2020). A review of internet of medical things (IoMT)—Based remote health monitoring through wearable sensors: A case study for diabetic patients. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(1), 414–422. Scopus. https://doi.org/10.11591/ijeecs.v20.i1.pp414-422

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ali, Z., Ahad, A., Madeira, F., & Shayea, I. (2024). Enhancing transparency and trustworthiness of healthcare IoT data with AWS: A proposed model. In V. Ferraro, M. Covarrubias, E. Zdravevski, I. M. Pires, J. M. Marques Martins De Almeida, & N. J. Gonçalves (Eds.), *IoT technologies and wearables for healthCare* (Vol. 530, pp. 44–56). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-71911-0_4

Almeida, V. A. F., Doneda, D., & Monteiro. (2015). *Governance challenges for the internet of things*. https://doi.org/10.1109/MIC.2015.86

Almeida, V. A. F., Goh, B., & Doneda, D. (2017). A principles-based approach to govern the IoT ecosystem. *IEEE Internet Computing*, *21*(4), 78–81. https://doi.org/10.1109/MIC.2017.2911433

Al-rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., & Zwiri, A. (2022). IoT adoption and application for smart healthcare: A systematic review. *Sensors*, *22*(14). https://doi.org/10.3390/s22145377

Alsadoon, A., Al-Naymat, G., & Jerew, O. D. (2024). An architectural framework of elderly healthcare monitoring and tracking through wearable sensor technologies. *Multimedia Tools and Applications*, *83*(26), 67825–67870. https://doi.org/10.1007/s11042-024-18177-0

Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). Internet of Things (IoT) communication protocols: Review. *2017 8th International Conference on Information Technology (ICIT)*, 685–690. https://doi.org/10.1109/ICITECH.2017.8079928

Anthopoulos, L., Janssen, M., & Weerakkody, V. (2016). A unified smart city model (USCM) for smart city conceptualization and benchmarking. *International Journal of Electronic Government Research (IJEGR)*, *12*(2), 77–93. https://doi.org/10.4018/IJEGR.2016040105

Aranha, H., Masi, M., Pavleska, T., & Sellitto, G. P. (2019). Securing mobile e-health environments by design: A holistic architectural approach. *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 1–6. https://doi.org/10.1109/WiMOB.2019.8923479

Aski, V. J., Dhaka, V. S., Kumar, S., & Parashar, A. (2022). IoT enabled elderly monitoring system and the role of privacy preservation frameworks in e-health applications. In D. J. Hemanth, D. Pelusi, & C. Vuppalapati (Eds.), *Intelligent data communication technologies and Internet of Things* (Vol. 101, pp. 991–1006). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-7610-9_72

AXELOS. (2019). *ITIL foundation, ITIL 4 edition*. Axelos. https://books.google.com/books?id=qW6-xwEACAAJ

Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, *5*, 26521–26544. Scopus. https://doi.org/10.1109/ACCESS.2017.2775180

Banda, G., Bommakanti, C. K., & Mohan, H. (2016). One IoT: An IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible. *Journal of Reliable Intelligent Environments*, *2*(3), 131–144. https://doi.org/10.1007/s40860-016-0027-5

Barroca Filho, I. D. M., & De Aquino Junior, G. S. (2018). A software reference architecture for IoT-based healthcare applications. In O. Gervasi, B. Murgante, S. Misra, E. Stankova, C. M. Torre, A. M. A. C. Rocha, D. Taniar, B. O. Apduhan, E. Tarantino, & Y. Ryu (Eds.), *Computational science and its applications – ICCSA 2018* (Vol. 10963, pp. 173–188). Springer International Publishing. https://doi.org/10.1007/978-3-319-95171-3_15

Berger, P., & Luckmann, T. (1966). The social construction of reality. In *Social theory re-wired* (3rd ed.). Routledge.

Birkle, C., Pendlebury, D. A., Schnell, J., & Adams, J. (2020). Web of Science as a data source for research on scientific and scholarly activity. *Quantitative Science Studies*, *1*(1), 363–376. https://doi.org/10.1162/qss_a_00018

Blobel, B. (2019). Challenges and solutions for designing and managing pHealth ecosystems. *Frontiers in Medicine*, *6*. https://doi.org/10.3389/fmed.2019.00083

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, *8*, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks* (No. NIST IR 8228; p. NIST IR 8228). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8228

Borse, Y., & Sharma, D. (2024). Blockchain based e-healthcare data sharing framework. *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 1–6. https://doi.org/10.1109/ICBDS61829.2024.10837499

Boyle, F., & Sherman, D. (2006). Scopus™: The product and its development. *The Serials Librarian*, *49*(3), 147–153. https://doi.org/10.1300/J123v49n03_12

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bygstad, B., & Iden, J. (2017). A governance model for managing lightweight IT. In Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *Recent Advances in Information Systems and Technologies* (Vol. 569, pp. 384–393). Springer International Publishing. https://doi.org/10.1007/978-3-319-56535-4_39

Chibuike, M. C., Grobbelaar, S. S., & Botha, A. (2024). Overcoming challenges for improved patient-centric care: A scoping review of platform ecosystems in healthcare. *IEEE Access*, *12*, 14298–14313. https://doi.org/10.1109/ACCESS.2024.3356860

Copie, A., Fortis, T. F., Munteanu, V. I., & Negru, V. (2013). From cloud governance to IoT governance. *Proceedings - 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013*, 1229–1234. https://doi.org/10.1109/WAINA.2013.169

Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research. In *Designing and conducting mixed methods research* (Third edition.). Sage.

Dang, X.-T., Knauer, R., Peters, S., & Sivrikaya, F. (2021). A converged cloud-fog architecture for future eHealth applications. *2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC)*, 1–8. https://doi.org/10.1109/FMEC54266.2021.9732552

Darshan, K. R., & Anandakumar, K. R. (2015). A comprehensive review on usage of Internet of Things (IoT) in healthcare system. *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, 132–136. https://doi.org/10.1109/ERECT.2015.7499001

Dasgupta, A., Gill, A., & Hussain, F. (2019). A conceptual framework for data governance in IoT-enabled digital IS ecosystems. *Proceedings of the 8th International Conference on Data Science, Technology and Applications*, 209–216. https://doi.org/10.5220/0007924302090216

Deutsches Institut für Normung. (2019). *DIN SPEC 91345:2016-04, referenzarchitekturmodell industrie 4.0 (RAMI4.0)*. DIN Media GmbH.

Elgammal, A., & Krämer, B. J. (2021). A reference architecture for smart digital platform for personalized prevention and patient management. In M. Aiello, A. Bouguettaya, D. A. Tamburri, & W.-J. van den Heuvel (Eds.), *Next-gen digital services. A retrospective and roadmap for service computing of the future: Essays dedicated to Michael Papazoglou on the occasion of his 65th birthday and his retirement* (pp. 88–99). Springer International Publishing. https://doi.org/10.1007/978-3-030-73203-5_7

ETSI. (2020). *EN 303 645—V2.1.1—CYBER; Cyber security for consumer internet of things: Baseline requirements*.

Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936. https://doi.org/10.1016/j.jnca.2020.102936

Firouzi, F., Farahani, B., & Marinšek, A. (2022). The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, *107*, 101840. https://doi.org/10.1016/j.is.2021.101840

Firouzi, F., Jiang, S., Chakrabarty, K., Farahani, B., Daneshmand, M., Song, J., & Mankodiya, K. (2023). Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine. IEEE Internet of Things Journal, 10(5), 3686–3705. https://doi.org/10.1109/JIOT.2022.3191881

Gardašević, G., Veletić, M., Maletić, N., Vasiljević, D., Radusinović, I., Tomović, S., & Radonjić, M. (2017). The IoT architectural framework, design issues and application domains. *Wireless Personal Communications*, *92*(1), 127–148. https://doi.org/10.1007/s11277-016-3842-3

General data protection regulation (GDPR) – legal text. (2025, June 8). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

George Ray, Ephais Ruhode, Albert Mubako, Jeff Ray, & Walter Kashiri. (2021). Security implications in the transformation of healthcare through internet of things devices. *Issues In Information Systems*. https://doi.org/10.48009/2_iis_2021_63-73

Gohar, A. N., Abdelmawgoud, S. A., & Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. *IEEE Access*, *10*, 92137–92157. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3202902

Grguric, A., Khan, O., Ortega-Gil, A., Markakis, E. K., Pozdniakov, K., Kloukinas, C., Medrano-Gil, A. M., Gaeta, E., Fico, G., & Koloutsou, K. (2021). Reference architectures, platforms, and pilots for european smart and healthy living—Analysis and comparison. *Electronics*, *10*(14), Article 14. https://doi.org/10.3390/electronics10141616

Gupta, D., Bansal, A., Wadhwa, S., & Shah, S. H. A. (2024). Fog-centric IoT smart healthcare: Architecture, applications, and case study. In N. K. Marriwala, S. Dhingra, S. Jain, & D. Kumar (Eds.), *Mobile radio communications and 5G networks* (pp. 123–131). Springer Nature. https://doi.org/10.1007/978-981-97-0700-3_9

Hajvali, M., Adabi, S., Rezaee, A., & Hosseinzadeh, M. (2022). Software architecture for IoT-based health-care systems with cloud/fog service model. *Cluster Computing*, *25*(1), 91–118. https://doi.org/10.1007/s10586-021-03375-4

Hasan, K., Chowdhury, M. J. M., Biswas, K., Ahmed, K., Islam, Md. S., & Usman, M. (2022). A blockchain-based secure data-sharing framework for software defined wireless body area networks. *Computer Networks*, *211*, 109004. https://doi.org/10.1016/j.comnet.2022.109004

Hasselgren, A., Hanssen Rensaa, J.-A., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2021). Blockchain for increased trust in virtual health care: Proof-of-concept study. *Journal of Medical Internet Research*, *23*(7), e28496. https://doi.org/10.2196/28496

He, A., Shen, J., Wang, Y., & Liu, L. (2018). Research on the fusion model reference architecture of sensed information of human body for medical and healthcare IoT. *2018 17th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, 162–164. https://doi.org/10.1109/DCABES.2018.00049

HL7 International. (2023, March 26). *Fast healthcare interoperability resources (FHIR) release 5.0.0: Overview*. Health Level Seven International. https://www.hl7.org/fhir/overview.html

Hu, F., Xie, D., & Shen, S. (2013). On the application of the internet of things in the field of medical and health care. *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2053–2058. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.384

Hussain, Md. I. (2017). Internet of Things: Challenges and research opportunities. *CSI Transactions on ICT*, *5*(1), 87–95. https://doi.org/10.1007/s40012-016-0136-6

IEEE. (2020). *IEEE standard for an architectural framework for the internet of things (IoT)*. https://doi.org/10.1109/IEEESTD.2020.9032420

Iftikhar, M., Tahir, S., Alquayed, F., & Hamid, B. (2023). Blockchain and LDP based smart healthcare IoT applications: Architecture, challenges and future

works. *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1–6. https://doi.org/10.1109/ICBATS57792.2023.10111134

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Islam, M. M., Hasan, M. K., Islam, S., Balfaqih, M., Alzahrani, A. I., Alalwan, N., Safie, N., Bhuiyan, Z. A., Thakkar, R., & Ghazal, T. M. (2023). Enabling pandemic-resilient healthcare: Narrowband Internet of Things and edge intelligence for real-time monitoring. *CAAI Transactions on Intelligence Technology*, *n/a*(n/a). https://doi.org/10.1049/cit2.12314

Ismail, S. F. (2017). IOE solution for a diabetic patient monitoring. *2017 8th International Conference on Information Technology (ICIT)*, 244–248. https://doi.org/10.1109/ICITECH.2017.8080007

ISO/IEC. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

ISO/IEC. (2022b). *ISO/IEC 27400:2022—Cybersecurity—IoT security and privacy guidelines*.

ISO/IEC. (2023). *ISO/IEC 27402:2023—Cybersecurity—IoT security and privacy—Device baseline requirements.*

ISO/IEC. (2024a). *ISO/IEC 30141 -I nternet of things (IoT) – Reference architecture*.

ISO/IEC. (2024b). *SO/IEC 27403:2024—Cybersecurity—IoT security and privacy—Guidelines for IoT-domotics.*

ISO/IEC. (2024c). *SO/IEC 27404—Cybersecurity—IoT security and privacy—Cybersecurity labelling framework for consumer IoT*.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods*, *18*(1), 3–20. https://doi.org/10.1177/1525822X05282260

Janbi, N., Mehmood, R., Katib, I., Albeshri, A., Corchado, J. M., & Yigitcanlar, T. (2022). Imtidad: A reference architecture and a case study on developing distributed AI services for skin disease diagnosis over cloud, fog and edge. *Sensors*, *22*(5), 1854. https://doi.org/10.3390/s22051854

Kabir, M. R., & Ray, S. (2024). DT-IoMT: A digital twin reference model for secure internet of medical things. *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 433–438. https://doi.org/10.1109/ISVLSI61997.2024.00084

Kakkar, A. (2019). *An IoT equipped hospital model: A new approach for E-governance healthcare framework*.

Kalingarani, G., & Selvaraj, P. (2022). Cognition based fog layer to mitigate the challenges of real-time medical applications. *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, 1–8. https://doi.org/10.1109/ICSES55317.2022.9914225

Kammueller, F. (2018). Formal modeling and analysis of data protection for GDPR compliance of IoT healthcare systems. *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 3319–3324. https://doi.org/10.1109/SMC.2018.00562

Keen, S., Lomeli-Rodriguez, M., & Joffe, H. (2022). From challenge to opportunity: Virtual qualitative research during COVID-19 and beyond. *International Journal of Qualitative Methods*, *21*, 16094069221105075. https://doi.org/10.1177/16094069221105075

Khan, S., Arslan, T., & Ratnarajah, T. (2022). Digital twin perspective of fourth industrial and healthcare revolution. *IEEE Access*, *10*, 25732–25754. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3156062

Khayat, M., Barka, E., & Sallabi, F. (2019). SDN_Based secure healthcare monitoring system(SDN-SHMS). *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 1–7. https://doi.org/10.1109/ICCCN.2019.8847097

Khowaja, S. A., Prabono, A. G., Setiawan, F., Yahya, B. N., & Lee, S.-L. (2018). Contextual activity based healthcare Internet of Things, Services, and People (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors. *Computer Networks*, *145*, 190–206. https://doi.org/10.1016/j.comnet.2018.09.003

Khther, R. A., & Othman, M. (2013). Cobit framework as a guideline of effective it governance in higher education: A review. *International Journal of Information Technology Convergence and Services*, *3*(1), 21–29. https://doi.org/10.5121/ijitcs.2013.3102

Kitchenham, B. (2004). *Procedures for performing systematic reviews*.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. *2*.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–93. https://doi.org/10.2307/249410

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

Kumar, G., Saha, R., Conti, M., Devgun, T., Goyat, R., & Rodrigues, J. J. P. C. (2023). COUNT: Blockchain framework for resource accountability in e-healthcare. *Computer Communications*, *209*, 249–259. https://doi.org/10.1016/j.comcom.2023.07.017

Kumar, M., Kavita, Verma, S., Kumar, A., Ijaz, M. F., & Rawat, D. B. (2022). ANAF-IoMT: A novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC. *IEEE Transactions on Industrial Informatics*, *18*(12), 8936–8943. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2022.3181614

Li, C., Wang, J., Wang, S., & Zhang, Y. (2024). A review of IoT applications in healthcare. *Neurocomputing*, *565*, 127017. https://doi.org/10.1016/j.neucom.2023.127017

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2017.2683200

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE.

Luo, S., & Ren, B. (2016). The monitoring and managing application of cloud computing based on Internet of Things. *Computer Methods and Programs in Biomedicine*, *130*, 154–161. https://doi.org/10.1016/j.cmpb.2016.03.024

M. Bublitz, F., Oetomo, A., S. Sahu, K., Kuang, A., X. Fadrique, L., E. Velmovitsky, P., M. Nobrega, R., & P. Morita, P. (2019). Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and internet of things. *International Journal of Environmental Research and Public Health*, *16*(20), Article 20. https://doi.org/10.3390/ijerph16203847

Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J. (2020). Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework. *Journal of Medical Internet Research*, *22*(9), e18623. https://doi.org/10.2196/18623

Mahammad, A. B., & Kumar, R. (2023). Scalable and security framework to secure and maintain healthcare data using blockchain technology. *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, 417–423. https://doi.org/10.1109/CISES58720.2023.10183494

Maina, A., & Singh, U. (2022). Exploring the scope of policy issues influencing IoT health and big data: A structured review. In A. Garg & D. P. Goyal, *Global Healthcare Disasters* (1st ed., pp. 123–144). Apple Academic Press. https://doi.org/10.1201/9781003282020-8

Memos, V. A., Psannis, K. E., Goudos, S. K., & Kyriazakos, S. (2021). An enhanced and secure cloud infrastructure for e-health data transmission. *Wireless Personal Communications*, *117*(1), 109–127. https://doi.org/10.1007/s11277-019-06874-1

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, *47*(7), 25–28. https://doi.org/10.1145/1005817.1005840

Mishra, P., & Singh, G. (2023). 6G-IoT framework for sustainable smart city: Vision and challenges. In P. Mishra & G. Singh, *Sustainable Smart Cities* (pp. 97–117). Springer International Publishing. https://doi.org/10.1007/978-3-031-33354-5_5

Muhammad, A. P., Akram, M. U., & Khan, M. A. (2015). Survey based analysis of internet of things based architectural framework for hospital management system. *2015 13th International Conference on Frontiers of Information Technology (FIT)*, 271–276. https://doi.org/10.1109/FIT.2015.54

Nanda, S. K., Panda, S. K., & Dash, M. (2023). Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimedia Tools and Applications*, *82*(21), 32917–32939. https://doi.org/10.1007/s11042-023-14846-8

Navaz, A. N., Serhani, M. A., El Kassabi, H. T., Al-Qirim, N., & Ismail, H. (2021). Trends, technologies, and key challenges in smart and connected healthcare. *IEEE Access*, *9*, 74044–74067. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3079217

Nguyen, Q. H., Dang, Q., Pham, C., Nguyen, T.-D., Nguyen, H., Setty, A., & Le, T. Q. (2020). Developing an architecture for IoT interoperability in healthcare: A case study of real-time SpO2 signal monitoring and analysis. *2020 IEEE International Conference on Big Data (Big Data)*, 3394–3403. https://doi.org/10.1109/BigData50022.2020.9378200

Niknejad, N., Ismail, W., Ghani, I., Nazari, B., Bahari, M., & Hussin, A. R. B. C. (2020). Understanding Service-Oriented Architecture (SOA): A systematic literature review and directions for further investigation. *Information Systems*, *91*, 101491. https://doi.org/10.1016/j.is.2020.101491

Nuguri, S. S., Karthik, K., Pusapati, V., Kambhampati, A., Bhamidipati, S. C., Calyam, A., Alarcon, M. L., & Calyam, P. (2023). Zeus: IoT-based healthcare data management security framework for remote patient monitoring. *Proceedings of the 2024 Workshop on Cybersecurity in Healthcare*, 93–100. https://doi.org/10.1145/3689942.3694748

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*. https://doi.org/10.1287/isre.2.1.1

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Peña, J. J. S., Vicente, E. F., & Ocaña, A. M. (2013). *ITIL, COBIT and EFQM: Can they work together? 4*(1).

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, *21*(4), 7–22. https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2

Pir, A., Akram, M. U., & Khan, M. A. (2015). Internet of things based context awareness architectural framework for HMIS. *2015 17th International Conference on E-Health Networking, Application & Services (HealthCom)*, 55–60. https://doi.org/10.1109/HealthCom.2015.7454473

Prasad, B., & Ramachandram, S. (2021). Decentralized privacy-preserving framework for health care record-keeping over hyperledger fabric. In G. Ranganathan, J. Chen, & Á. Rocha (Eds.), *Inventive communication and computational technologies* (Vol. 145, pp. 463–475). Springer Singapore. https://doi.org/10.1007/978-981-15-7345-3_39

Prasad, V. K., Bhattacharya, P., Maru, D., Tanwar, S., Verma, A., Singh, A., Tiwari, A. K., Sharma, R., Alkhayyat, A., Țurcanu, F.-E., & Raboaca, M. S. (2023). Federated learning for the internet-of-medical-things: A survey. *Mathematics*, *11*(1), Article 1. https://doi.org/10.3390/math11010151

Pratt, M. K. (2023, December 28). What is GRC? The rising importance of governance, risk, and compliance. *CIO*. https://www.cio.com/article/230326/what-is-grc-and-why-do-you-need-it.html

Preetham, S., R., Haq Nalband, A., Sachin U, Chaithanya V, & Ahmed, M. R. (2023). Securing 5G-enabled internet of medical things in healthcare: Vulnerabilities, threats, and architectural framework. *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 1–8. https://doi.org/10.1109/CSITSS60515.2023.10334074

Pulkkis, G., Karlsson, J., Westerlund, M., & Tana, J. (2017). Secure and reliable internet of things systems for healthcare. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, 169–176. https://doi.org/10.1109/FiCloud.2017.50

Quy, V. K., Hau, N. V., Anh, D. V., & Ngoc, L. A. (2022). Smart healthcare IoT applications based on fog computing: Architecture, applications and challenges. *Complex & Intelligent Systems*, *8*(5), 3805–3815. https://doi.org/10.1007/s40747-021-00582-9

Rahman, A., Wadud, M. A. H., Islam, M. J., Kundu, D., Bhuiyan, T. M. A.-U.-H., Muhammad, G., & Ali, Z. (2024). Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. *Scientific Reports*, *14*(1), 5297. https://doi.org/10.1038/s41598-024-55662-w

Ramson, S. R. J., Vishnu, S., & Shanmugam, M. (2020). Applications of internet of things (IoT) – an overview. *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 92–95. https://doi.org/10.1109/ICDCS48716.2020.243556

Rasmussen, M. (2006). The emergence of GRC as a discipline. *Al*. https://grc2020.com

Reidy, C., A'Court, C., Jenkins, W., Jani, A., Ramos, A., Morys-Carter, M., & Papoutsi, C. (2023). 'The plural of silo is not ecosystem': Qualitative study on the role of innovation ecosystems in supporting 'Internet of Things' applications in health and care. *DIGITAL HEALTH*, *9*, 20552076221147114. https://doi.org/10.1177/20552076221147114

Santos, D. F. S., Gorgônio, K. C., Perkusich, A., & Almeida, H. O. (2016). A standard-based and context-aware architecture for personal healthcare smart gateways. *Journal of Medical Systems*, *40*(10), 224. https://doi.org/10.1007/s10916-016-0580-8

Sawand, A., Djahel, S., Zhang, Z., & Naït-Abdesselam, F. (2014). Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring systems. *2014 IEEE/CIC International Conference on Communications in China (ICCC)*, 187–192. https://doi.org/10.1109/ICCChina.2014.7008269

Sawand, A., Djahel, S., Zhang, Z., & Naït-Abdesselam, F. (2015). Toward energy-efficient and trustworthy eHealth monitoring system. *China Communications*, *12*(1), 46–65. China Communications. https://doi.org/10.1109/CC.2015.7084383

Scalco, A., Flanigan, D., & Simske, S. (2021). Control systems cyber security reference architecture (RA) for critical infrastructure: Healthcare and hospital vertical example. *Journal of Critical Infrastructure Policy*, *2*(2), 125–145. https://doi.org/10.18278/jcip.2.2.7

Sedrati, A., Mezrioui, A., & Ouaddah, A. (2023). IoT-Gov: A structured framework for internet of things governance. *Computer Networks*, *233*. https://doi.org/10.1016/j.comnet.2023.109902

Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Applied Sciences*, *2*(1). https://doi.org/10.1007/s42452-019-1925-y

Shah, J. L., Bhat, H. F., & Khan, A. I. (2021). Integration of cloud and IoT for smart Shah, J. L., Bhat, H. F., & Khan, A. I. (2021). Integration of cloud and IoT for smart e-healthcare. In V. E. Balas & S. Pal (Eds.), Healthcare paradigms in the Internet of Things ecosystem (pp. 101–136). Elsevier. https://doi.org/10.1016/B978-0-12-819664-9.00006-5

Sharma, A., Choudhury, T., & Kumar, P. (2018). Health monitoring & management using IoT devices in a cloud based framework. *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 219–224. https://doi.org/10.1109/ICACCE.2018.8441752

Shumba, A.-T., Montanaro, T., Sergi, I., Fachechi, L., De Vittorio, M., & Patrono, L. (2022). Leveraging IoT-aware technologies and AI techniques for real-time critical healthcare applications. *Sensors*, *22*(19), Article 19. https://doi.org/10.3390/s22197675

Singh, K. D., Singh, P. D., Kaur, G., Lamba, V., Veeramanickam, M. R. M., & Khullar, V. (2024). The convergence of cloud, IoT, and artificial intelligence for intelligent systems. In P. D. Singh & M. Angurala, *Integration of cloud computing and IoT* (1st ed., pp. 365–379). Chapman and Hall/CRC. https://doi.org/10.1201/9781032656694-20

Singh, U. K., & Sharma, A. (2021). Cloud computing security framework based on shared responsibility models. In V. Bali, V. Bhatnagar, D. Aggarwal, S. Bali, & M. J. Diván, *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0* (1st ed., pp. 39–55). CRC Press. https://doi.org/10.1201/9781003146711-3

Sittón-Candanedo, I., Alonso, R. S., Corchado, J. M., Rodríguez-González, S., & Casado-Vara, R. (2019). A review of edge computing reference architectures and a new global edge proposal. *Future Generation Computer Systems*, *99*, 278–294. https://doi.org/10.1016/j.future.2019.04.016

St. Cyr, T. J. (2013). An overview of healthcare standards. *2013 Proceedings of IEEE Southeastcon*, 1–5. https://doi.org/10.1109/SECON.2013.6567436

Sulis, E., Cordero, A., Donetti, S., Ferrero, P., & Violato, A. (2021). A framework for project risk assessment in telehealth. *2021 IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 216–221. https://doi.org/10.1109/CHASE52844.2021.00043

Talaminos-Barroso, A., Reina-Tosina, J., & Roa, L. M. (2022). Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems. *Measurement: Sensors*, *22*, 100375. https://doi.org/10.1016/j.measen.2022.100375

Theodoridis, E., Mylonas, G., & Chatzigiannakis, I. (2013). *Developing an IoT smart city framework*. http://www.smartsantander.eu/map/

Tomashchuk, O., Van Landuyt, D., & Joosen, W. (2021). The architectural divergence problem in security and privacy of eHealth IoT product lines. *Proceedings of the 25th ACM International Systems and Software Product Line Conference - Volume A*, 114–119. https://doi.org/10.1145/3461001.3473061

Uslu, B. Ç., Okay, E., & Dursun, E. (2020). Analysis of factors affecting IoT-based smart hospital design. *Journal of Cloud Computing*, *9*(1), 67. https://doi.org/10.1186/s13677-020-00215-5

Valero, C. I., Gil, A. M. M., Gonzalez-Usach, R., Julian, M., Fico, G., Arredondo, M. T., Stavropoulos, T. G., Strantsalis, D., Voulgaridis, A., Roca, F., Jara, A. J., Serrano, M., Zappa, A., Khan, Y., Guillen, S., Sala, P., Belsa, A., Votis, K., & Palau, C. E. (2021). AIoTES: Setting the principles for semantic interoperable and modern IoT-enabled reference architecture for Active and

Healthy Ageing ecosystems. *Computer Communications*, *177*, 96–111. https://doi.org/10.1016/j.comcom.2021.06.010

Venčkauskas, A., Štuikys, V., Toldinas, J., & Jusas, N. (2016). A model-driven framework to develop personalized health monitoring. *Symmetry*, *8*(7), Article 7. https://doi.org/10.3390/sym8070065

Vijayakumaran, C., Muthusenthil, B., & Manickavasagam, B. (2020). A reliable next generation cyber security architecture for industrial internet of things environment. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(1), 387. https://doi.org/10.11591/ijece.v10i1.pp387-395

Wakili, A., & Bakkali, S. (2024). Ethical considerations in the integration of internet of things (IoT) technologies within digital health: A comprehensive framework for evaluation. In M. Ezziyyani, J. Kacprzyk, & V. E. Balas (Eds.), *International conference on advanced intelligent systems for sustainable development (AI2SD'2023)* (Vol. 905, pp. 219–231). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52385-4_21

Weber, R. H. (2013). Internet of things—Governance quo vadis? *Computer Law and Security Review*, *29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010

Weber, R. H. (2016). Governance of the internet of things—From infancy to first attempts of implementation? *Laws*, *5*(3), 28. https://doi.org/10.3390/laws5030028

Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud based wearable ECG monitoring system for smart healthcare. *Journal of Medical Systems*, *40*(12), 286. https://doi.org/10.1007/s10916-016-0644-9

Yusof, M. Mohd., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for Health Information Systems: Human, organization and technology-fit factors (HOT-fit). *International Journal of Medical Informatics*, *77*(6), 386–398. https://doi.org/10.1016/j.ijmedinf.2007.08.011

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 22–32. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2014.2306328