A Review of IoMT Security and Privacy Related Frameworks.

Ramadhan M. Rajab, Mabrouka Abuhmida, Ian D. Wilson and Richard P. Ward
University of South Wales, Pontypridd, United Kingdom

ramadhan.rajab@southwales.ac.uk
mabrouka.abuhmida@southwales.ac.uk
ian.wilson@southwales.ac.uk
richard.ward@southwales.ac.uk

Abstract: This paper reviews current IoMT security and privacy frameworks, highlighting their contributions towards addressing the challenges in the rapidly evolving domains of IoT and IoMT. It examines the role of international standardisation efforts and evaluates the effectiveness of existing frameworks in enhancing interoperability and ensuring secure, reliable medical data communication. It begins by contextualising IoT within the broader spectrum of Ubiquitous Computing and Machine-to-Machine communications, underscoring its transformative potential. The paper delves into specific IoT frameworks, like the Open IoT Framework by Sun and Memon (2017), which emphasises microservices architecture for scalable and interoperable platforms. Additionally, it covers unique IoMT frameworks, including the SaYoPillow for stress and sleep analysis and the EMRI framework for secure healthcare data communication.

Keywords: IoT (Internet of Things), IoMT (Internet of Medical Things), Interoperability, Frameworks

1. Introduction

The development and implementation of the Internet of Things (IoT) and Internet of Medical Things (IoMT) frameworks have the potential to revolutionise various industries, including healthcare (Maskeliūnas et al., 2019). The integration of artificial intelligence (AI) and IoT technologies has led to radical transformations in the healthcare industry, creating what is known as the Intelligent IoMT. Furthermore, the emergence of IoMT-based healthcare monitoring systems has enabled medical practitioners to remotely monitor and analyse real-time health data. However, despite the numerous benefits and advancements in IoT and IoMT frameworks, challenges still need to be addressed. For instance, there is often a lack of interoperability and coordination between different systems and stakeholders in the healthcare sector. The fragmentation and inadequate linkage between the Ministry of Information and Communications Technology and healthcare providers can hinder the effective implementation of IoT and IoMT frameworks (Pelekoudas-Oikonomou et al., 2022). Additionally, the lack of standardised protocols and interoperable functionalities in existing electronic medical record systems limits the exchange of patient data between healthcare facilities. As a result, there is a need for comprehensive and standardised frameworks that address these challenges and ensure the secure and efficient integration of IoT and IoMT technologies in the healthcare industry. To address these challenges, it is crucial to establish robust cybersecurity measures and protocols to protect patient data and ensure the privacy and confidentiality of sensitive healthcare information.

2. Literature Review

Existing IoMT frameworks and standards discussed in the literature include the E-Health Big Data Architecture (E-HBDA) (Villegas-Ch & García-Ortiz, 2023), the cov-AID framework (Hamid et al., 2022), and the Digital Forensic Investigation Framework (DFIF) (Hassan et al., 2022). The E-HBDA framework focuses on collecting, storing, and analysing data generated by IoMT devices, using Hadoop and Spark for data processing and analysis (Lin et al., 2022). The cov-AID framework is designed for remote monitoring, diagnosis, and prevention of COVID-19, utilising IoMT sensors and extensive data analysis (Hassan et al., 2022). The DFIF framework is used for digital forensic investigation in the IoT environment, addressing challenges in IoT security and providing solutions and strategies. These frameworks differ in their specific objectives and applications, with E-HBDA and cov-AID focusing on healthcare and COVID-19, respectively, while DFIF addresses digital forensic investigation in the IoT environment.

Existing IoMT frameworks and standards have evolved to address the challenges of heterogeneity, interoperability, and security in the healthcare sector. These frameworks provide functionalities such as data collection, storage, analysis, and decision-making based on machine learning models. They aim to improve the accuracy, reliability, and productivity of electronic equipment in healthcare. The frameworks also focus on ensuring the safety and transparency of data usage, as well as backtracking decisions made by medical professionals. Standardisation is crucial to increase trust and enable the integration of devices from different

vendors. The frameworks emphasise the need for common functionalities, interoperability standards, and network protocols across sectors. They also highlight the importance of openness, support for various applications, and the creation of healthy ecosystems in the IoT community (Mahalakshmi S.and Desai, 2022).

There are other proposed IoT frameworks that have been previously developed within the past decade. A previous instance is the Open IoT Framework by Sun et. al. (2017), that is based on Microservices Systems Architecture, that offers more scalable, extensive, interoperable, and maintainable platforms, that can accommodate heterogenous objects, and easily achieve application integration using automation, geo service intelligence and Big Data (Sun et al., 2017). This proposed framework coined the concept “Internet of Infinite Things”, a vision where everything in the world may communicate with each other (Sun et al., 2017).

The upcoming section will present architectures related to the Internet of Medical Things (IoMT) and outline several well-established frameworks.

3. IoMT Architectures and Frameworks

3.1 Microservice-Based Architectures for IoMT Scalability and Interoperability

Microservice architecture has emerged as a potential approach to enable scalable and interoperable systems for IoMT applications. In contrast to traditional monolithic architectures, microservices decompose a large system into a suite of independently deployable modular services. As discussed by Sun and Memon (2017), this brings key benefits for IoMT platforms that need to integrate heterogeneous devices, data, systems, and user interfaces. A microservice oriented IoMT platform implements functionalities as discrete services, and core capabilities are implemented in a central microservice.

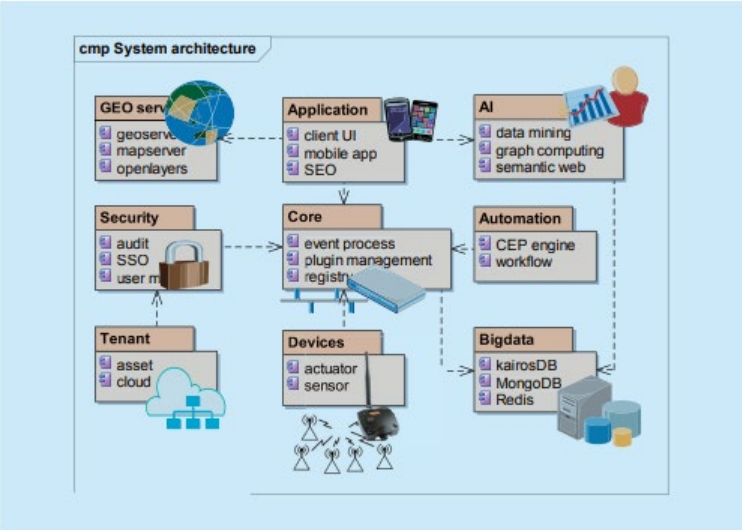

Figure 1: Microservice Based IoT Framework (Sun and Memon, 2017)

Sun and Memon (2017) propose a conceptual Open IoT microservice-oriented architecture for IoMT platforms, where specialised concerns such as geospatial capabilities, application modules, big data analytics, and machine learning are delegated to surrounding microservices. This approach enables independent development of various services in optimal languages with suitable data models, facilitating flexibility within the IoMT environment. Standard web interfacing architectures like the Representational State Transfer (REST) facilitate data exchange among services, while containerisation frameworks like Docker support testing and simulation of operational environments for individual microservices (Sun et al., 2017, p. x). **Figure 1** highlights the proposed architecture, which is composed of eight different microservices that are integrated to facilitate a flexible and interoperable IoT platform. It also has extensive features that may allow it to accommodate more of these microservices.

A key issue to be addressed here is distinguishing between IoT and IoMT application development architectures and frameworks, where application frameworks are shell abstractions that provide optimal solutions to software challenges (Mnkandla, 2009), as application architectures are sets of structures that formulate the disciplines and methods of developing applications (Perry & Wolf, 1992).

The SaYoPillow is an IoMT framework proposed by Rachakonda *et al.* (2021), that aims to understand the relationship between stress and sleep through an IoT edge device. The framework provides statistically monitored analysis to determine if the user has achieved sufficient and complete sleep in a day. **Figure 2** highlights specialised microservices for key functions. Note that it also monitors and controls psychological stress during the sleep period and in relation to food habits. The framework addresses several major issues identified by Rachakonda *et al.* (2021):

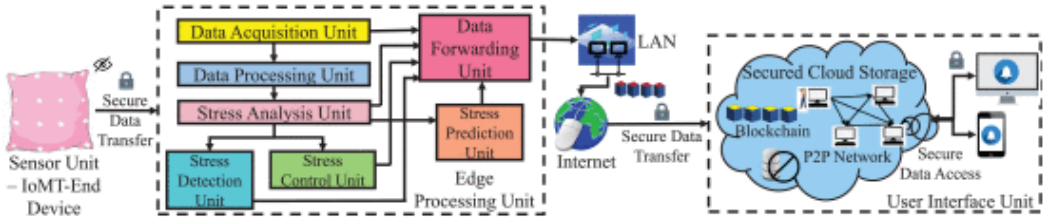

Figure 2: SaYoPillow Architecture (Rachakonda et al.,2021)

The SaYoPillow framework integrates a non-wearable device for stress monitoring during sleep, processing edge device data securely stored in the cloud. It enables stress detection, prediction, and user privacy in IoT cloud storage (Rachakonda et al., 2021. The cloud setup includes an EC2 Admin node, a miner, and two peers, with Geth clients on end-user devices accessing physiological data. Policy smart contracts on the admin node control user access, while RSA key encryption managed by a key system ensures secure client interactions. Prior to encryption, irreversible digests are generated using SHA-256 hashing, with digital signatures for data integrity (Rachakonda et al., 2021).

Ghubaish *et al.* (2020) proposed a security framework for mitigating various known physical and network related attacks. It was developed with reference to a four-layered IoMT system architecture, i.e., the sensor, gateway, cloud, and visualisation layers. It adopts certain features that provide three key functions, i.e. secure collection, transmission, and storage of data, based on the exploration, assessment, and analysis of the available security techniques, and how resilient they are against the IoMT attack surface, upon their findings indicating that no single technique can provide comprehensive security to IoMT systems against fourteen known IoMT physical and network related attacks (Ghubaish et al., 2020).

3.2 Blockchain Frameworks for IoMT Data Privacy and Security

Mallick and Sharma (2021) propose a Blockchain-based Electronic Medical Record Infrastructure (EMRI), facilitating secure communication and preserving patient data privacy. EMRI enables remote access to patient reports, addressing centralised Internet of Medical Things (IoMT) limitations. It employs smart contracts for privacy policy maintenance and Proof of Work (PoW) for block validation, ensuring decentralisation and reducing single points of failure. Smart contracts grant limited transaction access to non-trusted participants based on predefined policy terms. (Malick and Sharma, 2021). The EMRI algorithm occurs as follows:

- Doctor must be from a healthcare institution.
- Doctor must be a registered EMRI system user.
- Doctor logs in with user credentials.
- Smart contract is automatically executed.
- Patient provides Personal Identifiable Information (PII) for inputting medical data.
- Doctor provides treatment with reference to patient medical data.

According to the smart contract terms, validated user credentials, and verified PII, diagnostic centers add patient clinical records to a blockchain database, stored in decentralized ledger blocks validated by minor nodes. Hospitals operating these systems must adhere to regulatory authority guidelines, with registered practitioners. Smart contracts define terms for decentralized authentication of non-trusted parties. EMRI offers transparency and data integrity without modification, leveraging decentralized architecture for scalability, security, and privacy (Mallick & Sharma, 2021).

Golosova and Romanovs (2018) identified challenges in implementing blockchain technology in Emergency Medical Response Initiatives (EMRI), such as high energy consumption for real-time ledger maintenance, cryptographic complexities in signature verifications, and network instability from chain splits. Balancing node numbers and user costs remains problematic, with high rewards incentivizing nodes but potentially slowing

transaction processing. Node capacity limitations may compromise blockchain immutability and transparency, leading to centralization and security risks. Additionally, while smart contracts are immutable, they lack flexibility for necessary annulments, particularly in dynamic ecosystems. Concerns also arise regarding contractual secrecy and privacy breaches in public ledger environments.

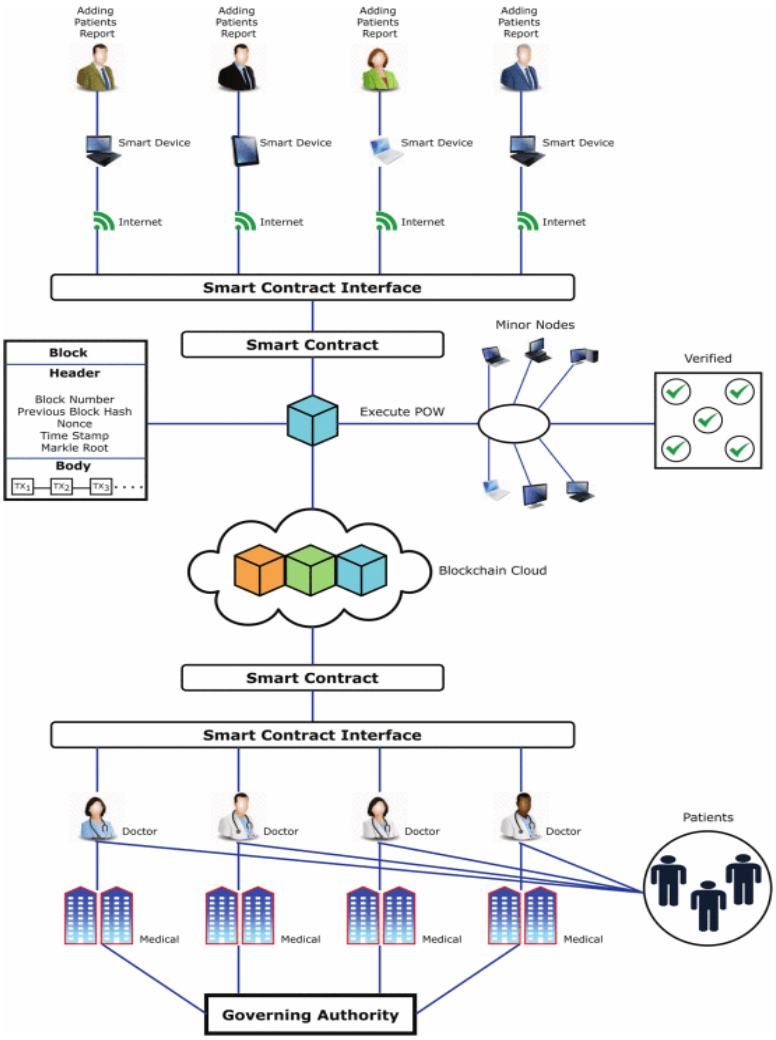

Figure 3: Process of Blockchain Smar Contracts (Rahmani et al.,2022)

The integration of secure protocols ensures transactional anonymity and guards against unauthorized access in blockchain systems. Legal adjudications encounter challenges in enforcing smart contract terms, particularly in the Internet of Medical Things (IoMT). Ongoing research focuses on trust management, cloud computing, and improving malware detection in IoMT devices. Innovations include energy-efficient solutions, merging 6G with 5G, integrating blockchain with edge computing and machine learning, and developing quantum-computing-based IoMT technologies (Nzuva, 2019 ; Rahmani et al., 2022). **Figure 3** depicts the proposed blockchain smart contract process (Rahmani et al., 2022).

4. IoMT Standards and Regulations

4.1 HL7 FHIR Standard for Healthcare Interoperability

Health Level 7 (HL7) is a non-profit organization accredited by the American National Standards Institute (ANSI), formulating ISO-accredited standards for exchanging electronic health information (HL7org, 2023). These standards provide a standardized framework crucial for clinical and medical management, outlining linguistic, structural, and typological requirements (HL7org, 2023). HL7's international presence involves affiliates dedicated to adapting standards globally, while in the United States, it operates through the U.S. Realm Steering Committee (HL7org, 2023). HL7 hosts 40 workgroups across healthcare sectors, overseen by elected co-chairs

and divided into four steering divisions, managed by the Technical Steering Committee and the HL7 Board of Directors (HL7org, 2023). The HL7 standards' categorization is detailed in Table 1 (McKenzie & Peters, 2022).

Table 1: HL7 Sections

HL7 SECTION		SECTION NAME
Section 1		Primary Standards
	Section 1a	Clinical Documentation Architecture (CDA)
	Section 1b	Electronic Health Records (EHR)
	Section 1c	Fast Healthcare Interoperability Resources (FHIR)
	Section 1d	Version 2 (V2)
	Section 1e	Version 3 (V3)
	Section 1f	Arden Syntax
	Section 1g	Clinical Context Management Specification (CCOW)
	Section 1h	Cross-paradigm/Domain Analysis Models
Section 2		Clinical and Administrative Domains
Section 3		Implementation Guides
Section 4		Rules and References

The HL7 standardization process typically involves a 2-year timeline for a specification to achieve "Standard Trial for Use" status, followed by 3 or more years for it to become normative, reflecting ANSI standards and maintaining backward compatibility through upgrades (McKenzie, 2022). Basic interactions like those outlined in **Table 2** are complemented by advanced interactions such as Batch/Transaction (CRUD operations), VRead, Patch, and Capabilities, along with operational interactions enabling actions like RPC paradigms. Additionally, endpoints encompass validation and documentation entities (Kryszyn et al., 2023).

Table 2: HL7 FHIR Process Commands

NAME	INTERACTION
Create	Create new resource with server id. = POST url/(resourceType)
Read	Reading current resource status. = GET url/{resourceType}/{id}
Update	Update an existing resource by id (or create new one). = PUT url/{resourceType}/{id}
Delete	Delete resource. = DELETE url/{resourceType}/{id}
Search	Search/filtering resources. = GET url/{resourceType}? Search parameters
History	Get the change history for specific resource. = GET url/{resourceType}/{id}/history

Kryszyn et al. (2023) suggests that the functionality of a server depends on its capabilities, leading to varying sets of interactions and resources to manage. Standard specifications facilitate extensions and resource profiles tailored to local requirements, particularly in data authorisation, access, and encryption scenarios.

4.2 Benefits of HL7 Standards

The benefits that HL7 brings into healthcare sector are as follows (McKenzie, 2022):

- Processes to help in forming communities, perform reviews and performing both testing and a balanced, objective review of specifications.
- A community of stakeholders with expertise in healthcare and data sharing technologies.
- A community with interests in technology to improve the flow of healthcare information.
- Processes at the outset of projects to ensure the scope is well defined, awareness of intended work propagated across the entire HL7 and external communities.
- Technical infrastructure to support communication, and knowledge sharing.
- Formal methodologies that guide creativity of consistent, good quality specifications.
- Regular connectivity, shared registries, and testing environments to support ongoing validation of specifications upon their development.

- Mechanisms to solicit review widely based on knowledgeable experts and processes to coordinate responses to adaptation and providing feedback.
- Management process to coordinate committee efforts and facilitate community processes.
- Governance process to ensure all stakeholders have an opportunity to express their opinions and specifications are developed collaboratively in due consensus.
- Regional affiliations and fostered partnerships with other standards-related organisations, regulatory authorities, and key stakeholders.

4.3 Limitations of HL7 Standards

There are limitations to HL7 standards which must be considered (McKenzie & Peters, 2022):

- Both the standards and implementer communities have finite bandwidth towards fulfilling project objectives, timelines, pending regulations, funding, and other critical considerations.
- While communal resources aim to be fairly allocated across work products, volunteers and funded members will only develop and review content that reflects their own interests.
- The difficult and time-consuming efforts towards the standards process is not the technical artifacts but working with the people.
- There are no guarantees in the outcomes, stability, timing, and adoption of the standard process.
- Standards contribute towards limited expectations. Significant change management is often needed to shift market incentives, business practices, professional cultures and habits, and regulations in ways that befit the benefits that are to be achieved by a specification.
- Considering that better outcomes are to be achieved gradually and incrementally, it takes a lot of effort and time to fulfil them.
- There are challenges in some respects towards HL7 interoperability with other organisational standards.

The Fast Healthcare Interoperability Resources (FHIR) framework prioritizes robust security and privacy measures. This includes encryption of communications, prevention of information leaks, mitigation against script injections, and establishment of audit trails. FHIR integrates NIST mobile device security and OWASP Top 10 and other standardised security frameworks. It also facilitates communication of individual preferences via standardised protocols, resource tagging for data sensitivity, and data access record sharing for disclosure accountability (HL7, 2011; Pulivarti, 2023).

Some common use cases and approaches towards implementing security and privacy controls using HL7 FHIR are highlighted in **Table 3**:

Table 3: HL7 FHIR Use Cases

FHIR USE CASE	DESCRIPTION
Authorisation and Access Control	Defined a security label infrastructure that supports access control management.
User Identity and Access Context	Implemented using OAuth and HL7 Smart App Launch.
Audit Logging and Provenance	Audit logs are essential when investigating system security related events with reference to their timestamps. Provenance records are essential in checking and auditing user activities within the system.
Privacy Consent	This is essential in legally and ethically directing the collection, use and disclosure of the health data of an individual.
Digital Signatures	These are provided and exist in reserved locations.
De-Identification, Pseudonymization and Anonymization	These data processes reduce privacy risks by modifying and eliminating elements to fit a specific use-case. This follows access control decisions allowing a form of de-identification of diagnostic test results for the requesting client, based on ISO/IEC 20889:2018 guidelines.
Labels	Provided to affect the handling of resources.
Data Management Policies	Defined set of data exchange capabilities that are appropriate and of legal use to ensure that regulations and requirements are met.
Narrative	This should be undertaken with care when extracted from FHIR resources.

FHIR USE CASE	DESCRIPTION
Input Validation	This received input of data must be acceptable and correct to ensure that it does not have content that may corrupt system operations.
Event Reporting	There should exist Legal and ethical obligations which must provide means of reporting security incidents.

A production FHIR system also has a security subsystem for user administration, authentication an authorisation that fits into a) the consumer using the healthcare system, b) the client application, c) the security system and d) a clinical/healthcare repository (HL7, 2023-b).

In the UK, particularly within England, NHS institutions have largely integrated HL7 standards, primarily driven by initiatives spearheaded by INTEROpen since 2018 (INTEROpen, 2023). INTEROpen, in collaboration with HL7 UK and FHIR stakeholders, introduced the Care Connect API approach to foster open standards for interoperability in healthcare and social care sectors (NHS England, 2021). The Care Connect API approach facilitates data communication and exchange across clinical centers at a national level, as outlined in the detailed development and deployment guideline provided in **Figure 4** (Care Connect, 2019).

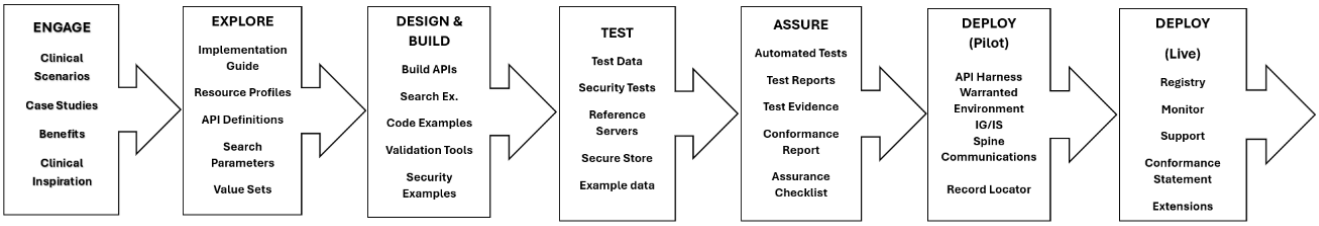

Figure 4: Guideline into developing a Care Connect API (Care Connect, 2019)

As from September 2021, the NHS Digital had strategized to adopt HL7 FHIR Release 4 to formulate a unified approach at UK National Level (N. H. S. England, 2019). The strategies move towards interoperability focuses upon:

- Working with services to identify strategic business needs.
- Developing priority use cases for interoperability to justify local business investment and development of supporting systems.
- Providing development support tools and guidance for interoperability to local institutions
- Developing electronic transfer standards for discharge from inpatient care and mental health.
- Accidental and Emergency attendance.
- Outpatient clinic letters.

According to the NHS England (2015), the interoperability of systems can be considerably achieved using two problematic approaches:

- **Technical interoperability** – This involves inter-systems processing of data based on the orchestration of reliable delivery of information (i.e., the "*how*")
- **Semantic interoperability** – This involves processing each system to ensure it understands and interprets the information it is processing without ambiguity, by use of specific coding and messaging schemes at the core of integrating health and social care (i.e., the "*what*")

As an approach to ensure the HL7 FHIR, and other key open standards that are implemented within public healthcare systems under NHS England, the National Information Board Interoperability Strategy was formed to develop Open APIs, as a requirement by the UK health and social care economy to self-assess the progress of its digital roadmap by April 2016 using a *Digital Maturity Index.* The key priority elements that were to be addressed by the Systems Interoperability strategy are the *NHS Number for every UK Citizen, Prescribed Medications for patients, NHS Medical Staff ID Numbers, Dates and Scheduling of Medical Appointments, Basic Observations on Patients upon their treatment, Basic Pathology* and *Diagnostic Coding* respectively (NHS England, 2015-b).

4.4 EU Regulations on Medical Device Safety and Security

The EU Medical Device Regulation (EU MDR), enacted in 2017, introduces stringent regulations, including expanded scope to diagnostic devices, higher risk classifications, and cybersecurity measures for IoMT devices.

Compliance challenges include complex approval processes, increased documentation, and costs affecting AI-based medical devices. IoMT devices face transitional issues adapting to the new regulations. While enhancing patient safety and device performance, the EU MDR poses challenges for manufacturers, impacting costs and product availability. It signals a significant shift in IoMT device security and AI development, prompting the need for more efficient clinical research methodologies and standardized protocols. (Vergani & Barrios, 2023;Melvin, 2022; Niemiec, 2022; Yu, 2021).

5. Challenges and Implications Around Security and Privacy of IoMT systems

In the current era of smart technology and IoT, securing IoMT devices in healthcare against cyber threats is crucial. Cybersecurity incidents, often due to human error, jeopardize patient data security, with diverse attack frequencies observed in the U.S. (Cartwright, 2023;Jiang & Bai, 2019). Notable incidents like the 2012 WannaCry attack underscore healthcare systems' vulnerability (Cartwright, 2023). Despite NHS efforts, ransomware attacks persist (Penfold, 2023). Legal frameworks like HIPAA, GDPR, and UK Data Protection Act emphasize robust cybersecurity (Memmi, 2023). Cyberattacks not only compromise patient safety but also raise ethical and financial concerns (Grably, 2022;Poulsen et al., 2021), with medical data fetching high values on the dark web (Sulleyman, 2017).

In Kenya, IoMT proliferation surpasses policy reforms, heightening ethical and security issues (Maina & Murungi, 2023). Inadequate national security standards exacerbate risks in E-Health (Raburu, 2021). Urgent regulatory actions are required (Maina & Murungi, 2023;Munyolo, 2021). Blockchain exploration faces regulatory hurdles, alongside challenges in EMR systems' interoperability and data confidentiality (Kamau et al., 2018). Collaborative efforts are essential to address IoMT cybersecurity risks and safeguard healthcare data integrity (Ondiek & Onyango, 2023). **Table 4** below comparatively summarises the challenges and implications in securing and assuring privacy in IoMT that are discussed in this section.

Table 4: Summary of the Challenges and Implications around IoMT security and privacy

IoMT Geographical Scope(s)	IoMT Challenge(s) Description	Implication to Challenge(s)	Author(s)
United States of America (USA)	Statistical investigations indicate diverse occurrences of cyber-attacks in healthcare, encompassing theft of Patient Health Data (41%), unauthorized access or disclosure (25%), hacking incidents (20%), data loss (10%), and improper disposal of records (3.4%).	Healthcare cyberattacks impact approximately 182 million patients. Breach frequency surged by 40% between 2018-2019, potentially exposing health data records.	Cartwright, 2023 Jiang & Bai, 2019
	Ransomware attack at Springhill Medical Centre in Alabama in 2019 affected a pregnant woman in labour.	cyberattack lead to the death of her baby nine months later.	Memmi, 2023; Poulsen et al., 2021
	There were 18 data breaches reported to the US Department of Health and Human Services Office for Civil Rights, rising to 368 by 2018, and 500 more data breaches in 2019, 347 more attacks in 2022.	Cyberattacks in healthcare pose significant risks to patient safety, particularly with patient-dependent Internet of Medical Things (IoMT) devices and systems.	Memmi, 2023; Poulsen et al., 2021
		Confirmation of 314,063,186 healthcare records were lost or stolen between 2009 and 2021.	Memmi, 2023
United Kingdom (UK)	Healthcare data, including Patient Health Information (PHI), is highly sensitive and regulated by laws like HIPAA, GDPR, and the UK Data Protection Act (2018) to ensure secure storage and access.	PHI's unique nature not only makes it a target for cyberattacks but also drives the development of cybersecurity solutions due to its critical role in patient care.	Memmi, 2023

IoMT Geographical Scope(s)	IoMT Challenge(s) Description	Implication to Challenge(s)	Author(s)
	NHS patient data can be traded on the dark web for financial ransom.	Data exfiltration, theft and exposure of healthcare data being traded at 10 times the value of bank data on the dark web.	Cartwright, 2023
	The WannaCry ransomware, affecting NHS 111 service and other systems.	This resulted into 20,000 cancelled medical appointments and operations, costing £92 million and jeopardising patient health, and affected MS Windows Computers in 80 NHS organizations.	Cartwright, 2023; Penfold, 2023
The Republic of Kenya	AI technologies were utilised to address service delivery challenges amid Covid-19 pandemic lockdowns.	There was limited digital preparedness due to financial constraints and infrastructural gaps raised ethical concerns regarding digital access.	Ondiek & Onyango, 2023
		Despite obstacles, Kenya deployed IoMT devices for Covid-19 monitoring, yet faced privacy issues due to insufficient implementation of proximity tracking, underscoring the necessity for ethical governance, privacy and transparency.	
	Cyberattacks on the E-Health in the Public Sector.	A loss of approximately $2 billion annually in revenue.	Raburu, 2021
	The technological progress has not standardized national security techniques. Healthcare faces challenges like manual processes, data quality issues, and inadequate security measures, hampering decision-making.	Challenges in the healthcare sector include manual processes, poor data quality, and insufficient data security measures, impeding effective decision-making.	Kamau et al., 2018
	The rapid growth of the Internet of Medical Things (IoMT) outpaces policy reforms, posing ethical and security risks and Stakeholder discrepancies hinder effective IoT policy engagement.	E-Health cyberthreats exceed defense mechanisms, jeopardising sensitive data.	Maina & Murungi, 2023; Munyolo, 2021
		There is limited access to healthcare forensics data from Kenya National Cybersecurity Incidence Response Team, which complicates the addressing of cyber-attacks.	
European Union (EU)	Corbeil-Essonnes Hospital in France was breached by Russian hackers and exfilrated healthcare data, exposing it on Google and the dark web, demanding a ransom of 10 million euros, later reduced to 1 million euros, which the hospital refused to pay.	Invested 2 million euros in system security and 5 million euros in cybersecurity upgrades, which is an incurring loss of revenue.	Memmi, 2023; Grably, 2022

6. Conclusion

This paper confirms that the examined frameworks pertaining to the IoMT exhibit certain identified flaws such as lack of scalability and immutability that impede their practical implementation into the real world. This is especially evident in the case of both the EMRI and SaYoPillow frameworks. Consequently, this justifies the need for further research with the aim of exploring more sophisticated approaches to developing scientifically agreeable and standardised technical security frameworks for IoMT, aside from relying on blockchain as a fundamental technical mechanism. There is also a crucial need to develop specific research, standards, and policies for ensuring cybersecurity and data privacy in the IoMT. Collaboration among healthcare, government, and technology stakeholders is essential to establish effective regulations and best practices. The vulnerability of the healthcare sector, attributed to legacy devices and disjointed data systems, emphasises the necessity for robust security risk assessment models to address challenges imposed within the rapidly evolving IoMT.

References

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, 1–10. https://doi.org/10.1007/s10877-023-01013-5

Connect, C. (2019). *Introduction to Care Connect API*. https://nhsconnect.github.io/CareConnectAPI/

England, N. (2023). *NHS England » Interoperability*. https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/interoperability/

England, N. H. S. (2015-a). *NHS England » Interoperability Handbook*. https://www.england.nhs.uk/publication/interoperabilty-handbk/

England, N. H. S. (2023-b). *NHS England » Procurement framework strategy recommendations*. https://www.england.nhs.uk/nhs-commercial/central-commercial-function-ccf/procurement-framework-strategy-recommendations/#minimum-standards

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet of Things Journal*, *8*(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653

Grably, R. (2022). 'Cyberattaque à l'hôpital de Corbeil-Essonnes: les données volées étaient accessibles par une simple...,'. *BFMTV*. https://www.bfmtv.com/tech/cybersecurite/cyberattaque-a-l-hopital-de-corbeil-essonnes-les-donnees-volees-etaient-accessibles-par-une-simple-recherche-google_AN-202210050374.html

Hamid, S., Bawany, N. Z., Sodhro, A. H., Lakhan, A., & Ahmed, S. (2022). A Systematic Review and IoMT Based Big Data Framework for COVID-19 Prevention and Detection. In *Electronics (Switzerland)* (Vol. 11, Issue 17). MDPI. https://doi.org/10.3390/electronics11172777

Hassan, M. A., Samara, G., & Fadda, M. A. (2022). IoT Forensic Frameworks (DFIF, IoTDOTS, FSAIoT): A Comprehensive Study. *International Journal of Advances in Soft Computing and Its Applications*, *14*(1), 72–86. https://doi.org/10.15849/IJASCA.220328.06

HL7. (2023-a). *FHIR Security*. https://www.hl7.org/fhir/security.html

HL7. (2023-b). *FHIR Security and Privacy Module*. https://www.hl7.org/fhir/secpriv-module.html

HL7org. (2023). *Introduction to HL7 Standards | HL7 International*. https://www.hl7.org/implement/standards/index.cfm?ref=nav

Jiang, J. X., & Bai, G. (2019). Evaluation of causes of protected health information breaches. *JAMA Internal Medicine*, *179*(2), 265–267. https://doi.org/10.1001/jamainternmed.2018.5295

Kamau, G., Boore, C., Maina, E., & Njenga, S. (n.d.). May. Blockchain technology: Is this the solution to emr interoperability and security issues in developing countries? *2018 IST-Africa Week Conference (IST-Africa*, 1. https://ieeexplore.ieee.org/abstract/document/8417357

Kryszyn, J., Smolik, W. T., Wanta, D., Midura, M., & Wróblewski, P. (2023). Comparison of OpenEHR and HL7 FHIR Standards. *International Journal of Electronics and Telecommunications*, 47–52. https://doi.org/10.24425/ijet.2023.144330

Lin, C., Zhuang, J., Feng, J., Li, H., Zhou, X., & Li, G. (2022). Adaptive Code Learning for Spark Configuration Tuning. *Proceedings - International Conference on Data Engineering*, *2022-May*, 1995–2007. https://doi.org/10.1109/ICDE53745.2022.00195

Mahalakshmi S. and Desai, K. (2022). IoT Framework, Architecture Services, Platforms, and Reference Models. In J. M. and S. S. Nandan Mohanty Sachi and Chatterjee (Ed.), *Internet of Things and Its Applications* (pp. 37–59). Springer International Publishing. https://doi.org/10.1007/978-3-030-77528-5_2

Maina, A., & Murungi, D. (2023). The Health Policy Implications of Social Representations of the Internet of Things in Kenya. *Academy of Management Proceedings (Vol. 2023*, *1*, 15849. https://doi.org/10.5465/AMPROC.2023.15849abstract

Mallick, S. R., & Sharma, S. (2021). EMRI: A scalable and secure Blockchain-based IoMT framework for healthcare data transaction. *19th OITS International Conference on Information Technology (OCIT*, 261–266. https://doi.org/10.1109/OCIT53463.2021.00060

Maskeliūnas, R., Damaševičius, R., & Segal, S. (2019). A review of internet of things technologies for ambient assisted living environments. *Future Internet*, *11*(12), 259.

McKenzie, L. (2022). *Understanding the standards Process" - HL7 - confluence (2022*. https://confluence.hl7.org/display/HL7/Understanding+the+Standards+Process

McKenzie, L., & Peters, M. (2020). *Participating in HL7 - HL7 - confluence - 2020"*. https://confluence.hl7.org/display/HL7/Participating+in+HL7

Melvin, T. (2022). The European Medical Device Regulation–What Biomedical Engineers Need to Know. *IEEE Journal of Translational Engineering in Health and Medicine*, *10*, 1–5. https://doi.org/10.1109/JTEHM.2022.3194415

Memmi, G. (2023). Cyber-attacks in healthcare: why they matter and how to defend against them. *British Journal of Healthcare Management*, *29*(1), 8–11. https://doi.org/10.12968/bjhc.2022.0134

Mnkandla, E. (2009). About software engineering frameworks and methodologies. In *AFRICON 2009* (pp. 1–5). IEEE. https://doi.org/10.1109/AFRCON.2009.5308117

Munyolo, G. N. O. (2021). *Cyber-security in E-health: a Critical Analysis of the Regulatory Framework in Kenya*. http://erepository.uonbi.ac.ke/bitstream/handle/11295/157251/Munyolo_Cyber-security%20in%20E-health.pdf?sequence=1

Navakauskas, D., Romanovs, A., Plonis, D., (2018) Institute of Electrical and Electronics Engineers. Lithuania Section, Institute of Electrical and Electronics Engineers. Latvia Section, Vilniaus Gedimino technikos universitetas, Rīgas Tehniskā universitāte, Institute of Electrical and Electronics Engineers. Lithuania Section. Education Society Chapter, & Institute of Electrical and Electronics Engineers. (2018). *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) : proceedings of the 6th IEEE workshop : November 8-10, 2016, Vilnius, Lithuania*.

Niemiec, E. (2022). Will the EU Medical Device Regulation help to improve the safety and performance of medical AI devices? *Digital Health*, *8*, 20552076221089080. https://doi.org/10.1177/20552076221089079

Nzuva, S. (2019). Smart contracts implementation, applications, benefits, and limitations. *Journal of Information Engineering and Applications*, *9*(5), 63–75. https://doi.org/10.7176/JIEA

Ondiek, J. O., & Onyango, G. (2023). Ethical Dilemmas in Public Innovations and ICT Solutions During COVID-19 in Kenya". In G. Onyango (Ed.), *Public Policy and Technological Transformations in Africa. Information Technology and Global Governance*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-18704-9_16

Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2022). Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. *Sensors*, *22*(7), 2449. https://doi.org/10.3390/s22072449

Penfold, J. (2023). The growing risk of cyber-attacks in the NHS. *British Journal of Healthcare Management*, *29*(1), 5–7. https://doi.org/10.12968/bjhc.2022.0132

Perry, D. E., & Wolf, A. L. (1992). Foundations for the study of software architecture. *ACM SIGSOFT Software Engineering Notes*, *17*(4), 40–52. https://doi.org/10.1145/141874.141884

Poulsen, K., McMillan, R., & Evans, M. (2021). *A hospital hit by hackers, a baby in distress: the case of the first alleged ransomware death*. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116?mod=hp_lead_pos5

Pulivarti, R. (2023). *Cybersecurity of Genomic Data*. https://doi.org/10.6028/NIST.IR.8432

Raburu, E. E. (2021). A Cybersecurity Model for the Health Sector: A Case Study of Hospitals in Nairobi, Kenya. http://erepo.usiu.ac.ke/11732/6742

Rachakonda, L., Bapatla, A. K., Mohanty, S. P., & Kougianos, E. (2021). SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits. *IEEE Transactions on Consumer Electronics*, *67*(1), 20–29. https://doi.org/10.1109/TCE.2020.3043683

Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): a systematic review. *Computational Intelligence and Neuroscience*. https://doi.org/10.1155/2022/9766844

Statement, Interopen. (2022). *United Kingdom*. https://www.intersystems.com/uk/resources/interopen-statement/

Sulleyman, A. (2017). 'NHS cyber-attack: Why stolen medical information is so much more valuable than financial data | The Independent,'. *The Independent*. https://www.independent.co.uk/tech/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

Sun, L., Li, Y., & Memon, R. A. (2017). An open IoT framework based on microservices architecture. *China Communications*, *14*(2), 154–162. https://doi.org/10.1109/CC.2017.7868163

Vergani, T., & Barrios, C. F. M. (2023). *Needs, Challenges, and Obstacles in the Implementation of the EU Medical Device Regulation*. https://www.iicj.net/subscribersonly/23june/iicj1jun-regulation-tancredivergan-obelis-belgium.pdf

Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics (Switzerland)*, *12*(18). https://doi.org/10.3390/electronics12183786

Yu, H. (2021). Digital health technologies under the new EU Medical Devices Regulation: monitoring and governing intended versus actual use. *BMJ Innovations*, *7*(4). https://doi.org/10.1136/bmjinnov-2021-000713