GMR
The Original

SECURE AND INTELLIGENT HEALTHCARE SYSTEMS WITH IOMT: BLOCK CHAIN AND INTEROPERABILITY CHALLENGES

Bidyutmala Saha[1*], Arun Kumar Majumdar[2], and Debapriya Roy [3]

[1]Department of Centre for Data Science, JIS Institute of Advanced Studies and Research (JISIASR), JIS University, India GNIT, Kolkata,India
[e-mail: sahabidyutmala1989@gmail.com]
[2]Department of Centre for Data Science, JIS Institute of Advanced Studies and Research (JISIASR), JIS University Kolkata,India [e-mail: majumdararunk@gmail.com]
[3]Department of Centre for Data Science, JIS Institute of Advanced Studies and Research (JISIASR), JIS University Kolkata,India [e-mail: debapriya.roy@jisiasr.org]

ABSTRACT
As a result of the rapid development of digital technologies within the healthcare field, the industry is now taking advantage of intelligent medical systems to monitor patients continuously and make data-based clinical decisions. The deployment of the Internet of Medical Things (IoMT), artificial intelligence advanced healthcare information system have greatly improved the productivity and access to the delivery of healthcare services today compared to what they were previously. However, while these technologies are increasing productivity and providing greater access to healthcare, they also create significant challenges concerning cyber security, data privacy, systems compatibility, and scalability due to the growing amount of connected medical devices and data-sharing platforms employed within the healthcare industry. New standards such as Fast Healthcare Interoperability Resources (FHIR) and new technologies such as block chain have been created to address these issues. These new standards and technologies facilitate secure data-sharing, greater transparency, and the ability to have fluid communication across different healthcare systems. Many studies have been conducted on these individual topics; however, most studies have focused on singular topics and do not provide an integrated approach to the three areas of security, interoperability, and intelligent decision-making. In this paper, we will review the latest literature on block chain-based healthcare systems, cyber security practices, and interoperability frameworks recognized within artificial intelligence (AI)-enabled IoMT healthcare environments. We also discuss the limitations of current approaches, including difficulties in real-world implementation, high computational cost, and legal and regulatory issues. The results of this study provide useful directions for future research to build secure, scalable, and interoperable intelligent healthcare systems.

KEYWORDS: Internet of Medical Things (IoMT); Artificial Intelligence; Blockchain Technology; Healthcare Cybersecurity; Interoperability; Fast Healthcare Interoperability Resources (FHIR).

1. INTRODUCTION

Healthcare systems will be profoundly affected by digital technologies. Digital solutions can have numerous advantages for both patients and providers. One significant development in modern healthcare has been the introduction of an emerging concept known as IoMT. IoMT describes a networked ecosystem of medical applications, and sensors. These networks are connected to the internet so that data can be exchanged among devices and applications over the internet. Various devices deploy cloud computing and artificial intelligence to facilitate real-time communication and continue to monitor patients continuously. Wearable medical devices such as smart watches, health bands, and remote monitoring sensors may now be considered key components of IoMT. Using these types of devices enables healthcare providers to monitor the status of their patients on a recurring basis without requiring their patients to be physically present for evaluation or treatment. Technology has improved how and when patients can receive healthcare services, how quickly new diseases can be identified, and the ability of healthcare providers to deliver individualized care (Olawumi et al. 2026).

With the increasing popularity of connected medical devices and digital health platforms, there also are multiple security/technical challenges. The Internet of Medical Things (IoMT) generates large amounts of data from a variety of sources such as wearable sensors; electronic health records (EHRs), medical imagery systems, and hospital databases. Properly managing and integrating this data is very complex, requiring an excellent system for sharing data, standardized methods of communication, and a scalable computing infrastructure (Carmona et al. 2026). To address this challenge, many healthcare interoperability standards based on Fast Healthcare Interoperability Resources (FHIR) are in place. These standards enable different healthcare systems and applications to share data with ease to support efficient collaborative behaviors. While interoperability is improving significantly, fully achieving interoperability continues to

be a significant challenge due to differences in format used by member organizations as well as ongoing use of legacy systems, and different types of semantic differences in the data (Olawumi et al. 2026). In addition to the challenges associated with IoMT-based healthcare interoperability, cyber security is another significant concern. The availability of many connected devices and systems on the network creates a growing risk of cyber attacks on IoMT-based healthcare systems. The healthcare industry is particularly vulnerable to cyber attacks due to the highly sensitive nature of health information. As a result, healthcare organizations need to ensure the confidentiality, integrity, and availability of patient data while protecting against the increased risk of being compromised through cyber attacks. There are various ways to enhance trust and enable secure data storage, including utilizing emerging technologies such as block chain technology. Block chain technology has the potential to create a distributed ledger that securely stores data is trustless, decentralized, readily accessible, and easily verifiable (Karbassi Yazdi et al. 2026). As a result, block chain may be used to improve healthcare data security, create accurate records, and facilitate secure data exchanges within today's healthcare systems. However, incorporating block chain into these systems will present challenges associated with scalability, computational overhead, and regulatory compliance.

AI has also become a game-changer in healthcare analytics, revolutionizing predictive modelling (e.g. predicting patients at risk for a disease), anomaly detection, clinical decision support and automating medical diagnosis (Tamizharasi et al. 2026). Machine learning and deep learning algorithms have shown great promise in the analysis of complex healthcare dataset to extract patterns of disease progression and patient risk profile. On the other hand, these emerging AI technologies can raise concerns in healthcare systems such as explainability of model reliability, computational complexity and operate effectively using resource limited Internet of Medical Things (IoMT) (Karbassi Yazdi et al. 2026). While many studies have investigated AI-based healthcare monitoring systems, cybersecurity frameworks, interoperability standards and blockchain-based health care architectures, current solutions do still mostly address these challenges independently (Carmona et al. 2026). Hence, the existing healthcare research is severely limited by the absence of robust, integrated frameworks that can adequately address security, interoperability, scalability and intelligent data analytics in one cohesive solution (Olawumi et al. 2026). Thus, this review paper investigates the state-of-the-art innovations in AI-assisted IoMT healthcare systems that concatenate cybersecurity mechanisms and interoperability standards with blockchain technologies for secure and smart healthcare monitoring (Chaudhary et al. 2025). The current study provides a comprehensive review of existing digital health care systems and their corresponding limitations. The following research gaps were found: difficulties in real-world application of systems; issues with protecting patient data privacy/protection; issues with handling large amounts of health care data; and the use of different platforms for the interoperable use of health care data. All of these issues create great challenges in developing a fully secure and effective digital health care system that provides all the functions necessary to provide quality care to patients (Karbassi Yazdi et al. 2026). The overall goal of these systems is to promote the development of digital health care systems that are more secure, connected, scalable, and intelligent in order to provide reliable patient services, protect patient data, and facilitate communication between medical devices and health care services.

2. METHODOLOGY

2.1 Search Strategy:

The research studies utilized within this paper were searched, analyzed, and collected systematically utilizing a list of keywords to locate papers associated with artificial intelligence (AI), internet of medical things (IoMT), cyber security in healthcare, block chain-supported healthcare systems, and a few interoperability frameworks (such as the fast healthcare interoperability resources or FHIR). The primary aim of the keyword list search was to collect the most recent and credible literature related to newly develop intelligent healthcare systems, security obstacles, and technical solutions used in today's digital healthcare (Obaid and Salman 2022). The systematic literature search was conducted using many of the most respected databases including IEEE Xplore, Scopus, Web of Science, Science Direct, Pub Med, and Google Scholar. These databases were selected because of their provision of peer-reviewed, high-quality research in computer science, healthcare informatics, and biomedical engineering. In addition, to keep the literature review focused on the most up-to-date digital healthcare technology advancements, the literature reviewed came from 2020 to 2026 (Olawumi et al. 2026)(Karbassi Yazdi et al. 2026). To complete the search, several simple processes were used. First, the titles and abstracts were reviewed to determine if they matched the subject of the literature review. After determining possible subject relevance, the full text for each of the eligible articles was carefully reviewed to identify methodology, contribution, and limitation of each article.

More importance was given to research related to IoMT-based healthcare architectures, AI-supported patient monitoring systems; cyber security frameworks in healthcare, interoperability standards, and block chain based healthcare solutions (Al-Fuqaha et al. 2015). In addition, the reference lists of the selected papers were also examined manually to find other useful studies that were not included in the initial database search. With this process, important research trends, gaps, and new challenges in intelligent healthcare systems were identified (Karbassi Yazdi et al. 2026).

2.2 Inclusion & Exclusion Criteria:

The inclusion-exclusion criteria of study publications provided a way to filter study publications that would be included in this review based on the extent to which studies were similar to the study objectives as they were limited in their inclusion criteria to published peer-reviewed journal articles or conference proceedings from recognized academic databases. The criteria were used to determine if the studies would be included, or excluded, from the final publication list (Imrie et al. 2025). The primary areas of research represented by the papers selected were AI, IoMT and healthcare

security issues, block chain based healthcare systems, and frameworks to support the interoperability among healthcare systems, including Fast Healthcare Interoperability Resources (FHIR); (Carmona et al. 2026). The studies included in this review proposed, analyzed, or evaluated the technical solutions required to create secure health systems, remote patient monitoring or intelligent infrastructure for healthcare. In an effort to maintain consistency and clarity in the interpretation of the research, the review included only those studies published in the English language; by selecting studies based on their relevance to current digital healthcare technologies, the review is intended to incorporate the most recent results related to intelligent and secure healthcare systems. Furthermore, the review only used papers published within the years of 2020-2026 in order to provide the most recent information regarding developments made in digital healthcare technology. Finally, the review only assessed papers with adequate methodological or technical details to support a viable critical review of the research. The review excluded the following types of publications:

i. Editorials, opinion articles, blog posts and news reports not subjected to peer review.
ii. Research with no clear focus on healthcare technologies, IoMT systems or healthcare data security.
iii. Articles with insufficient technical, methodological or analytical information.
iv. Duplicate publications found in several databases.
v. Literature addressing domains of application unrelated to healthcare.

2.3 Data Extraction and Analysis:

The selected parameters from each individual study were systematically extracted and analysed according to the inclusion and exclusion criteria. Specifically, this step aimed to ensure that relevant information from each paper was systematically gathered for a thorough collection and comparison of various works in the field of intelligent healthcare systems (Olawumi et al. 2026). For every paper that was selected, the key information including publication data, research aim, proposed technology or framework, application domain(s), datasets used along with evaluation methods and its findings were extracted. It is important for the studies to clearly define each technology component they used, including AI algorithms, IoMT system architecture, block chain based security mechanisms, and standards for interoperability standards such as IFC (FHIR). Also documented in detail by the authors were limitations of their studies, the challenges that were encountered while conducting the research and gaps in the existing literature. All paper data reviewed during this time period were examined using qualitative synthesis methods. There have been four general topic areas that have been identified from papers reviewed in the first phase of research: solutions for AI-based health monitoring based solutions; solutions to secure IT infrastructure with cyber security; solutions to use block chain to secure the storage and management of data, and solutions to facilitate the exchange of data between health care organizations. These four general areas were used for the systematic comparative analysis of the four different approaches to AI-enabled IoMT and provided a foundation for developing a systematic approach to identify each sample's strengths and weaknesses, identify and describe common challenges the researchers faced, identify emerging research trends and identify gaps in current literature. Based on the analysis of all reviewed studies, the current level of maturity for the technologies assessed was determined, and it was determined that more research is needed in certain areas. The structure of this review identifies the research already done on AI based IoMT healthcare systems and suggests potential future avenues of research (Carmona et al. 2026).

2.4 Paper Selection Process (PRISMA Description):

Description of the Process for Paper Selection This paper selection process in this review was conducted according to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement which is a set of items designed to promote transparent, reproducible, systematic identification of eligible studies. PRISMA has four stages identification, screening, eligibility and study inclusion (Karbassi Yazdi et al. 2026).

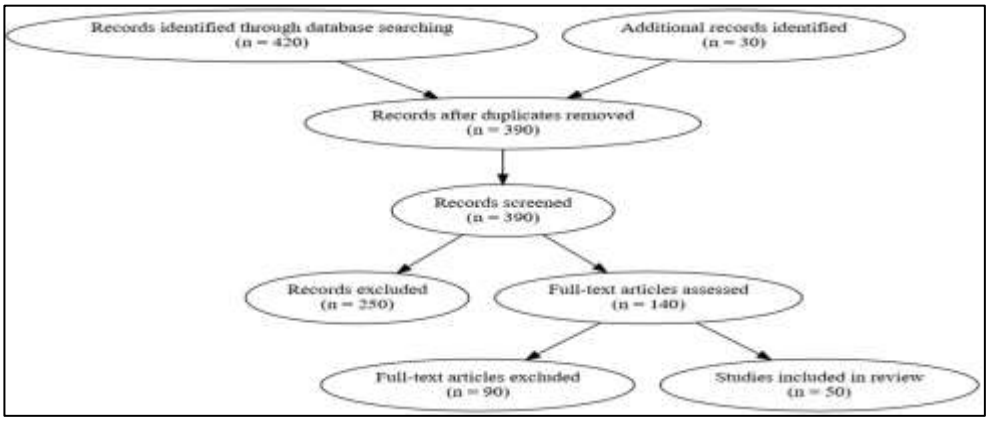

Fig 1. PRISMA Diagram

i. In regard to the identification phase, pertinent publications were retrieved from various academic databases like IEEE Xplore, Scopus, Web of Science, Science Direct, PubMed and Google Scholar with specific search keywords

related to artificial intelligence in healthcare (AI), Internet of Medical Things (IoMT), cyber security in healthcare and blockchain in health which includes interoperability frameworks including fast interoperability resources (FHIR). This search resulted in a wide-array of records from these databases (Jayant et al. 2024).

ii. In the screening phase, duplicate records retrieved from multiple databases were removed. These remaining articles were then assessed for relevance to the aims of this review by title and abstract screening (Karbassi Yazdi et al. 2026). At this point, any studies not directly related to IoMT healthcare systems, security or interoperability of such systems as well as intelligent healthcare technologies was excluded.

iii. In the eligibility phase, full texts of all remaining articles were reviewed to determine whether these studies met our predefined inclusion and exclusion criteria. Papers were excluded when they did not provide enough technical detail, did not focus on relevant domains, or the contribution was not a meaningful addition to the research topic. (Wong et al. 2023) Finally, in the inclusion stage, the studies which met all eligibility criteria were included in the final review (Obaid and Salman 2022). The papers were further reviewed to understand their methods, contributions, limitations and research gaps. We performed a PRISMA-based selection process with an eye towards producing a structured and bias-free review focusing on relevant literature in AI-enabled IoMT healthcare systems and affiliate technologies that support them (Imrie et al. 2025).

3. Historical Background:

3.1 Literature review:

Digital health information systems have evolved in conjunction with developments in information and communications technologies. Traditionally, healthcare service providers have operated their backend systems on the basis of manual record keeping and less information sharing mechanisms that led to unnecessarily separated patient profile data-points and inefficient clinical workflows. (Olawale and Ebadinezhad 2024) Electronic Health Records (EHRs) have revolutionized the way patient data are stored, managed and exchanged among healthcare providers. EHR systems were a boon for accessibility of patient information, clinical documentation, and more informed medical decision-making (Olawumi et al. 2026). With the continuous advancement of health care technologies, Internet of Things (IoT) technologies broke into the medical field giving rise to what we refer today as the Internet of Medical Things (IoMT). IoMT describe a system of medical devices and applications that connect to healthcare IT systems through online computer networks, connecting various wearable sensors as well (Jayant et al. 2024). This data is very useful for knowing the physiological conditions of people and carrying out monitoring in order to reveal abnormalities (Karbassi Yazdi et al. 2026). At the start, IoMT applications were introduced in the form of basic remote patient monitoring systems that enabled continuous monitoring of cardiovascular and glucose parameters (Hady et al. 2020). Due to the growing integration of technologies like wireless communication, cloud computing, and sensor technology, IoMT systems developed over time and became platforms for continuous health monitoring. Due to the fast growth of healthcare data from IoMT devices, there was a need for advanced data analysis tools to interpret and utilize this vast amount of data properly.

When each of these providers is utilizing a different data format and information system, the smooth flow and sharing of data becomes a challenge; and as a result of such fragmentation, the establishment of standard data exchange frameworks has become essential (Jayant et al. 2024). To this end, several interoperability frameworks have been developed as defined standards for the seamless sharing and transfer of information between disparate healthcare systems, with one example being Fast Healthcare Interoperability Resources (FHIR). Additionally; with increasing interest in using block chain technology in various healthcare applications due to the need for secure data storage and reliable sharing methods, the growing number of stakeholders utilizing the health data system leads to more ways that block chain technology can further enhance the healthcare industry. As a result, the availability of highly secure health data is a considerable challenge, as block chain technology operates on a decentralized basis to enhance data transparency, security and trustworthiness among users accessing the data; however, many practical challenges still exist when implementing block chain solutions within the healthcare space, including but not limited to scalability issues, regulatory compliance issues, computational cost concerns, and delays in data processing (Tamizharasi et al. 2026)(Hady et al. 2020).

3.2 Research Gaps:

While there have been many advancements in digital health technologies over recent years there continues to remain significant barriers to the successful implementation/integration of intelligent health care technologies. Advances have occurred with the emergence of technologies such as the Internet of Medical Things (IoMT), block chain technology, and interoperability Frameworks that have allowed for improved monitoring of patients and management of patient health data, however, their practical implementation within actual health care practice remains limited. This limitation arises primarily due to the lack of proper integration among technical systems/organizational policies/regulatory requirements that exist within health care organizations. An application of these barriers/challenges is vital for future research and the development of more dependable and secure health care infrastructure (Shaik et al. 2024).

3.2.1 Data Privacy Risks: As health care systems maintain a large amount of sensitive information related to patients they present themselves as highly attractive targets to cyber-attackers. Cyber-attacks against health care systems include example of ransom ware cyber-attack, data breaches, and unauthorized access to a network or systems. With the rapid growth of connected IoMT devices, health care networks have become increasingly vulnerable to cyber-attacks due

to the increased number of potential attack points across the health care environment. Currently, many of the existing security solutions available in the marketplace only protect at the network level and therefore do not provide adequate protection at the device level, enabling more secure device authentication, or enabling real-time threat detection. The distributed and interconnected nature of healthcare environments makes it extremely difficult to develop robust cyber security frameworks capable of protecting the entire health care infrastructure (Obaid and Salman 2022).

3.2.2 Interoperability and Data Integration Issues: Even though standards such as Fast Healthcare Interoperability Resources (FHIR) were introduced to solve interoperability problems, differences in implementation and the continued use of old legacy systems still create many difficulties. (Kayalvizhi et al. 2023) Sharing healthcare information between hospitals, laboratories, and other institutions becomes complicated because of differences in data structure, communication protocols, and organizational policies.

3.2.3 Real-World challenges: In terms of computational complexity and scalability, large amounts of real-time health data resulting from wearable devices, monitoring devices and medical imaging devices create major challenges for IoMT (Internet of Medical Things) systems (Obaid and Salman 2022). These systems must have a sufficient amount of computational power to process and analyse the amount of data that they're generating, however the majority of AI-based healthcare models being established are built using complex deep learning architectures which creates challenges when deployed in real-time on resource-constrained IoMT devices (Olawumi et al. 2026). As a result, scalability is a major open research problem when developing scalable AI-based healthcare systems. Additionally, the limited amount of real-world deployment and validation makes it difficult to validate the performance, reliability and user acceptability of intelligent medical devices in real-time because there is not a strong body of published literature to support these claims (Schouten et al. 2025). Most of the literature surrounding the use of intelligent medical devices is based on controlled environments, observational studies or retrospective analyses; therefore there is limited knowledge of operational barriers associated with large scale implementations of intelligent medical devices (Chaudhary et al. 2025).

To conclude, although intelligent healthcare systems can truly transform the provision of medical services, overcoming issues relating to security, interoperability, scalability, real-world deployment and regulatory compliance will be critical for their successful adoption (Bonagiri et al. 2024). Data anonymization for privacy-preserving federated learning in healthcare will eventually lead to the design of these holistic solutions, providing strong, trusted, patient-centric systems powered with cutting-edge technology (Hady et al. 2020).

3.3 Future Perspectives: Digital health technologies have developed rapidly and are transforming healthcare systems globally. Innovative technologies such as artificial intelligence, Internet of Medical Things (IoMT), blockchain, and cloud computing and next-level data interoperability frameworks will reportedly support the development of future healthcare infrastructures (Olawumi et al. 2026). Although current science has shown the powers of such technologies, future works will focus on system integration, scalability, security and use-cases (Imrie et al. 2025). An important line of future research includes designing more efficient and lightweight AI models to work with resource absent IoMT environments. Most of the current AI-based healthcare models are based on complex deep learning architectures that demand extremely high computational power. Moreover, future studies may involve models that are optimized and trained on such edge nodes, as well as federated learning techniques where the underlying model will learn via the local healthcare data without compromising a given patient privacy (Sharma et al. 2022).

As a second avenue, we have interoperability frameworks which improve the systems for exchanging data between healthcare organisations. Healthcare systems of the future must be able to implement normalized and scalable solutions capable of aggregating data from a myriad of sources including electronic health records, wearables, medical imaging systems and laboratory information systems.(Wong et al. 2023) Improved interoperability standards like FHIR, along with their assimilation in advanced data integration technologies will facilitate better collaborative care. Furthermore, blockchain technology is predicted to receive increasing leapfrog in secure healthcare data management. In the future, research may investigate blockchain designs that are more scalable with lower computational and energy footprints while still providing a strong data integrity and transparency guarantees (Kayalvizhi et al. 2023). In addition, new health care systems will probably stress real-world deployment and clinical validation of novel technologies (Al-Fuqaha et al. 2015). Only large scale pilot implementations and interdisciplinary collaborations among healthcare professionals, researchers, developers of technological systems will translate thousands of theoretical models into practical instances for real world situations of health care (Wong et al. 2023).

4. Comparative Study:

Ref.	Study / Paper	Main Objective	Key Technologies	Dataset / Method	Key Contributions	Limitations
(Ol	RemoteCare: AI-	Develop a	CNN, GRU,	WUSTL-	Provides dual-task	Evaluated on a
awu	Driven	multimodal	LSTM,	EHMS-	prediction for	single dataset;
mi	Multimodal	framework for	SHAP	2020	health status and	limited real-
et	Predictive	personalized	Explainable	dataset	cyberattack	world
al.	Framework with	health	AI,		detection;	deployment;
202	Blockchain for	monitoring and	Blockchain,		integrates	high
6)	Personalized	cyberattack	IPFS		explainable AI and	computational

	Remote Patient	detection in			blockchain-based	complexity;
	Monitoring in	IoMT			logging	blockchain
	IoMT	environments				scalability
						concerns
(Ca	A	Review	Encryption,	Scoping	Provides broad	Lacks
rmo	Comprehensive	cybersecurity	Zero-Trust	review	overview of	experimental
na	Survey of	threats, privacy	Architecture,	using	cybersecurity risks	evaluation;
et	Cybersecurity	risks, and	Blockchain,	PRISMA-	and mitigation	limited IoMT-
al.	Threats and Data	mitigation	AI-based	ScR	strategies in	specific threat
202	Privacy Issues in	strategies in	threat	methodolo	healthcare systems	analysis;
6)	Healthcare	healthcare	detection	gy		minimal
	Systems	systems				quantitative
						comparison of
						solutions
(Ka	FHIR in Focus:	Examine the	FHIR APIs,	Systematic	Highlights the	Implementatio
rbas	Enabling	role of FHIR	EHR	review	importance of	n variability
si	Biomedical Data	in healthcare	systems, AI	across	standardized	across
Yaz	Harmonization	data	integration,	healthcare	interoperability	institutions;
di et	for Intelligent	interoperability	cloud	implement	frameworks for	integration
al.	Healthcare	and integration	platforms	ations	healthcare data	challenges with
202	Systems				exchange	legacy systems;
6)						security and privacy
						concerns
(Ta	Innovating	Explore	Blockchain,	Expert-	Identifies potential	Based on
miz	Mental	blockchain	Electronic	based	applications of	expert opinion
hara	Healthcare with	applications	Health	Delphi	blockchain in	rather than
si et	Blockchain	and barriers in	Records,	study (45	mental health data	practical
al.	Technology:	mental	Delphi	experts)	management and	implementation
202	Expert	healthcare	method		patient	; limited
6)	Perspectives	systems			empowerment	geographic
	from Tanzania					scope;
						infrastructure
						and regulatory
						challenges

5. RESULT COMPARISON

The review of literature presented here sets the ground for discussion with respect to selected studies was based on comparisons showing strength and limitation of intelligent healthcare system in addressing research challenges. Scores were awarded across several key technological categories such as AI capability, security mechanisms, interoperability support, scalability and real world validation (Mittal et al. 2022). The analysis showed that AI powered healthcare frameworks show reliable predictive healthcare monitoring and anomaly detection abilities.(Tamizharasi et al. 2026) For example, in analyzing physiological data received from IoMT devices AI-based architectural frameworks using deep learning models provides high accuracy[51]. Nevertheless, these methods require the use of complex models that are time-consuming to run and therefore may be difficult to deploy in low-resourced health care settings (Jayant et al. 2024).

Numerous studies surrounding healthcare security highlight the importance of safeguarding sensitive patient data from cyber attacks. A variety of techniques, such as encryption techniques, intrusion detection systems, and block chain-based systems, have been proposed to ensure the safety and accuracy of patient records. While all of these methods increase overall security, most of them remain mostly experimental and untested in the real-world setting of healthcare (Rasheed and Kumar 2025). Interoperability frameworks based on recognized guidelines have been said to offer a significant benefit by facilitating seamless data exchange among healthcare networks. The interoperability framework allows electronic health record data, wearable technology data, and clinical data to be combined into a single unified healthcare information system. However, despite the substantial advantages offered by interoperability frameworks, adoption has been led by differences in methodology and challenges with integrating legacy systems (Olawale and Ebadinezhad 2024). The visual representation of these data allows for easy analysis and comparison of the different methodologies based on their efficiency, practicality, and overall technological feasibility (Schouten et al. 2025).

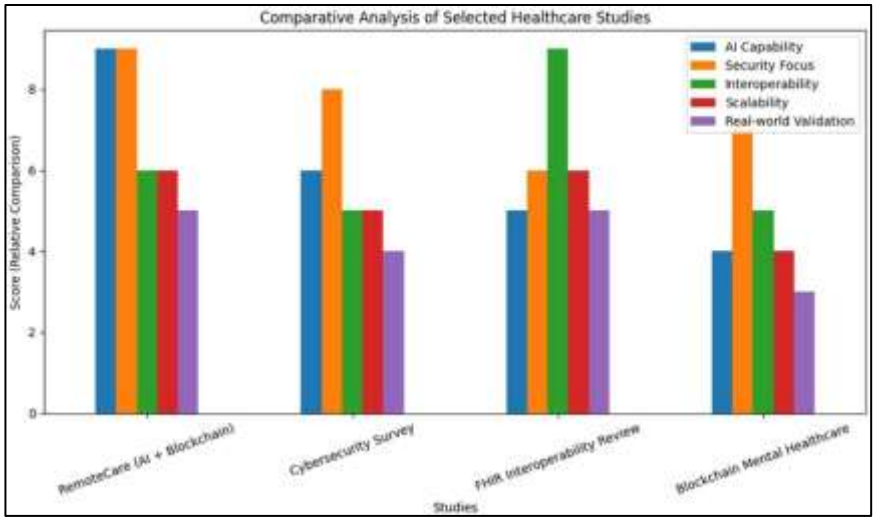

Fig 2. Comparative Analysis

Figure 2 provides a comparison of some of the selected healthcare studies, based on system intelligence; system capability; system security; system interoperability; system scalability; and the extent to which the systems were tested in a real-world setting. The Remote Care framework has performed exceptionally well in both system capability and system security, whereas the FHIR interoperability review demonstrates significantly superior performance in the areas of data sharing and system compatibility (Kore and Patil 2022). One of the studies considered focuses primarily on cyber security-related issues whereas a second study discussed uses Block chain technology for data protection; however, both of these studies have not been validated in real-life healthcare systems (Hady et al. 2020).

Figure 3 compares the various studies with a radar chart through the parameters of system capability, security, interoperability, scalability, and real-world use. Remote Care demonstrates good performance in system capability and system security. The study based upon FHIR demonstrates strong interoperability support; whereas, several of the other studies do not cover multiple areas, either focusing on security or data management in their entirety. This indicates that future healthcare systems need comprehensive and integrated solutions that are able to meet multiple requirements/needs simultaneously. In conclusion, the results of comparing the aforementioned studies collectively indicate that future healthcare systems should include a combination of features such as robust security, seamless data exchange; scalability; and practical implementations in actual settings (Kore and Patil 2022).

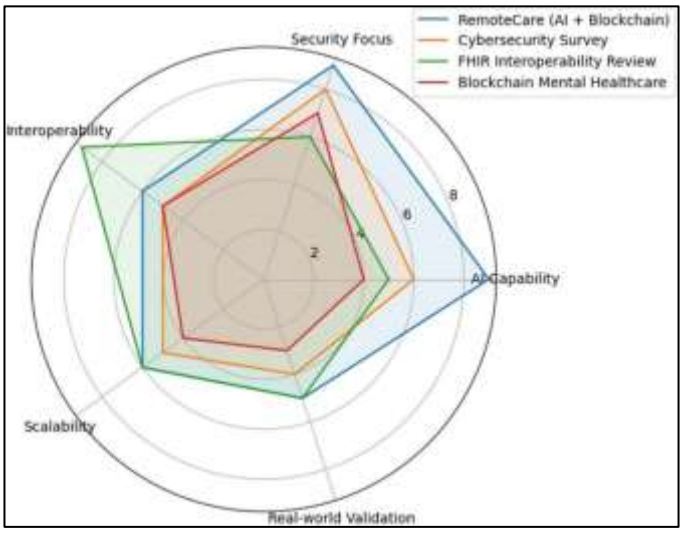

Fig 3. Radar Comparison

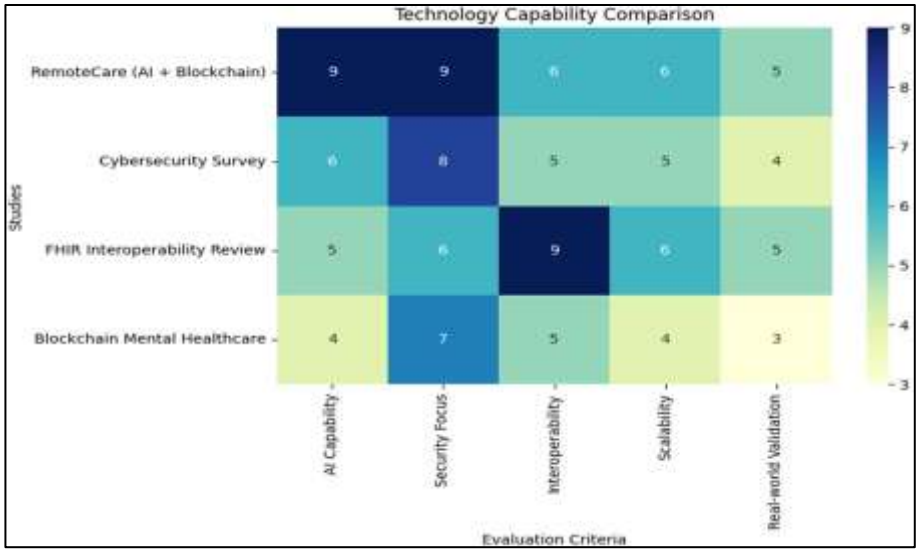

Fig 4. Technology Capability Comparison

We compare the selected studies as detailed in Fig. 4, and use a heatmap to present AI capability, focus on security or interoperability, scalability and validation against real-world data.(Mhiri et al. 2024)(Gupta et al. 2024) As seen in the visualization, Remote Care ranks high on both AI capability and security, while FHIR interoperability review also scores strongest in interoperability. The cybersecurity survey had a focus on security and the blockchain mental healthcare study seems to have low scores in comparison across most categories. Summary, results show that advance will be reached only in integration of care if the health solution in design focused on more than just one tech dimension (Mittal et al. 2022).

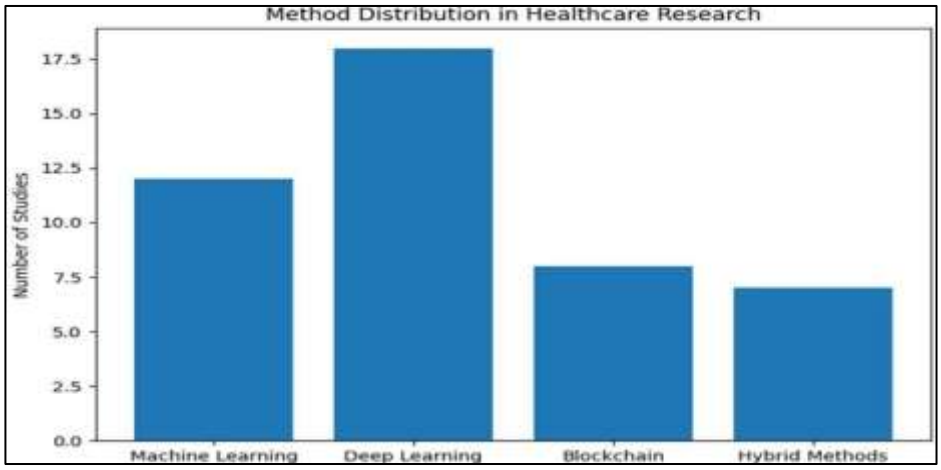

Fig 5. Method Distribution Chart

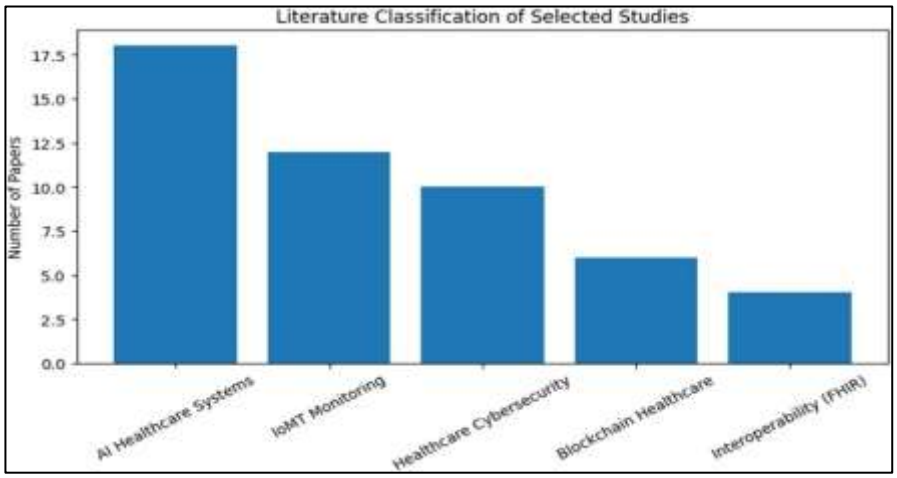

Fig 6. Literature Classification Graph

6. CONCLUSION

Today's intelligent healthcare systems are experiencing gradual success through systematic improvement, yet continued barriers limiting their broad adoption have been identified as some of the most fundamental issues. Difficulties experienced during actual implementation pose varying challenges to the development of intelligent healthcare systems that utilize standardized clinical terminologies concerned with cyber security and data protection. The interoperability required for heterogeneous healthcare systems based on current standards. There are many existing studies that rely heavily on small sample sizes, thus making assessment of the perceived efficacy of each proposed solution in actual clinical environments difficult. The principal issue that continues to impede progress towards developing advanced smart healthcare systems is the current absence of formalized standards to facilitate integration of multiple technologies into a single unified healthcare infrastructure, thereby necessitating a need for more thorough and actionable research. One more common challenge is that there are no standards-based frameworks available that provide for the incorporation of multiple technologies into a unified healthcare delivery infrastructure. This need for comprehensive, practical research requires comprehensive investigation into what constitutes an advanced, integrated, secure and scalable smart healthcare architecture. In addition, there is a requirement for logical designs of architectures that are both intrinsically secure and can be built at scale in order to support large volumes of medical data while providing safety, reliability, and efficiency.

Successfully meeting these various challenges will lead to the establishment of reliable, effective, and patient-centric digital healthcare infrastructures, and will ultimately support the long-term growth of sustainable and intelligent healthcare systems.

REFERENCE

1. 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. DOI: https://doi.org/10.1109/COMST.2015.2444095
2. Bonagiri K., Nici Marx V.S., Gopalsamy M., Iyswariya A., Reni Hena Helan R., Sultanuddin
3. S.J. 2024. AI-driven healthcare cyber-security: protecting patient data and medical devices.
4. p. 107–112. In: Proceedings of the 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI). 28–30 August 2024, Coimbatore, India. DOI: https://doi.org/10.1109/ICoICI62571.2024.10819243
5. Carmona P.M., Sosa-Sánchez E., Clemente P.J. 2026. TrackpathDSL: Petri Net-based supply chains towards blockchain services. Blockchain: Research and Applications. DOI: https://doi.org/10.1016/j.bcra.2026.100452
6. Chaudhary A., Khullar V., Kaushik K. 2025. Guest editorial: advancing personalized healthcare integrating AI and health informatics. IEEE Journal of Biomedical and Health Informatics 29 (7): 4597–4598. DOI: https://doi.org/10.1109/JBHI.2025.3583282
7. Gupta K., Saxena D., Rani P., Kumar J., Makkar A., Singh A.K., Lee C.N. 2024. An intelligent quantum cyber-security framework for healthcare data management. IEEE Transactions on Automation Science and Engineering 22: 6884–6895. DOI: https://doi.org/10.1109/TASE.2024.3525008
8. Hady A.A., Ghubaish A., Salman T., Unal D., Jain R. 2020. Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access 8: 106576–106584. DOI: https://doi.org/10.1109/ACCESS.2020.3000819
9. Imrie F., Denner S., Brunschwig L.S., Maier-Hein K., van der Schaar M. 2025. Automated ensemble multimodal machine learning for healthcare. IEEE Journal of Biomedical and Health Informatics 29 (6): 4213–4226. DOI: https://doi.org/10.1109/JBHI.2025.3554732
10. Jayant P., Vincent E., Mohana M., Moharir M., Kumar A.R.A. 2024. Smart health monitoring and anomaly detection using Internet of Things (IoT) and artificial intelligence (AI). p. 479–485. In: Proceedings of the 2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI). August 2024. DOI: https://doi.org/10.1109/ICoICI62571.2024.10819695
11. Karbassi Yazdi A., Tan Y., Khoobbakht M.A., González G.V., Ocampo L. 2026. Blockchain technology for green supply chain management in the maritime industry: integrating extended grey relational analysis, SWARA, and ARAS methods under Z-information. Mathematics 14 (2): 246. DOI: https://doi.org/10.3390/math14020246
12. Kayalvizhi S., Nagarajan S., Deepa J., Hemapriya K. 2023. Multimodal IoT-based medical data processing for disease diagnosis using heuristic-derived deep learning. Biomedical Signal Processing and Control 85: 104889. DOI: https://doi.org/10.1016/j.bspc.2023.104889
13. Kore A., Patil S. 2022. Cross-layered cryptography based secure routing for IoT-enabled smart healthcare system. Wireless Networks 28: 287–301. DOI: https://doi.org/10.1007/s11276-021-02844-9
14. Mhiri S., Egio A., Compastié M., Cosio P. 2024. Proxy re-encryption for enhanced data security in healthcare: a practical implementation. p. 1–11. In: Proceedings of the 19th International Conference on Availability, Reliability and Security. 30 July–2 August 2024, Vienna, Austria. DOI: https://doi.org/10.1145/3664476.3670453
15. Mittal S., Bansal A., Gupta D., Juneja S., Turabieh H., Elarabawy M.M., Bitsue Z.K. 2022. Using identity-based cryptography as a foundation for an effective and secure cloud model for e-health. Computational Intelligence and Neuroscience 2022: 7016554. DOI: https://doi.org/10.1155/2022/7016554
16. Obaid O.I., Salman S.A.-B. 2022. Security and privacy in IoT-based healthcare systems: a review. Mesopotamian Journal of Computer Science 2022: 29–39. DOI: https://doi.org/10.58496/MJCSC/2022/007

17. Olawale O.P., Ebadinezhad S. 2024. Cybersecurity anomaly detection: AI and Ethereum blockchain for secure and tamperproof IoHT data management. IEEE Access 12: 131605–131620. DOI: https://doi.org/10.1109/ACCESS.2024.3465900
18. Olawumi T.O., Ojo S., Muftaudeen S.T., Odeh A.O., Amoo T. 2026. Assessing blockchain technology's technical utility in construction supply chains: a multi-KPI decision support approach via use cases. Computers in Industry. DOI: https://doi.org/10.1016/j.compind.2025.104429
19. Rasheed A.M., Kumar R.M.S. 2025. Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. Frontiers in Computer Science 7: 1522184. DOI:
20. https://doi.org/10.3389/fcomp.2025.1522184
21. Schouten D., Verma A., Möller M., Hering A., Truhn D., Haubold J., Kuhl C.K., Kather J.N., Kleesiek J., Nensa F. 2025. Navigating the landscape of multimodal AI in medicine: a scoping review on technical challenges and clinical applications. Medical Image Analysis 105: 103621. DOI: https://doi.org/10.1016/j.media.2025.103621
22. Shaik T., Tao X., Li L., Xie H., Velasquez J.D. 2024. A survey of multimodal information fusion for smart healthcare: mapping the journey from data to wisdom. Information Fusion 102: 102040. DOI: https://doi.org/10.1016/j.inffus.2023.102040
23. Sharma P., Moparthi N.R., Namasudra S., Shanmuganathan V., Hsu C.H. 2022. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. Expert Systems 39: e12915. DOI: https://doi.org/10.1111/exsy.12915
24. Tamizharasi G.S., Arjun K.P., Sathiyaraj R., Balusamy B., Khan F., Khadidos A.O., Selvarajan S. 2026. Blockchain intelligence empowered secure uncertainty management in IoT-assisted smart grids. Cluster Computing 29: 166. DOI: https://doi.org/10.1007/s10586-026-05984-3
25. Wong G.X., Tung Yew H., Diargham J.A., Wong F., Mamat M., Chung S.K. 2023. IoMT real-time health monitoring system. p. 269–273. In: Proceedings of the 12th International Conference on Awareness Science and Technology (iCAST). November 2023. DOI: https://doi.org/10.1109/iCAST59866.2023.10461618