

UNPACKING ETHICAL, PRIVACY, AND GOVERNANCE RISKS IN AI-IOT BASED HEALTHCARE ENVIRONMENTS: A THEMATIC ANALYSIS

Joana Jaya¹, Asmat Ara Shaikh^{*2}, Pankaj Sahu³, B.Mahalakshmi⁴, Olina Jaya¹

1. Faculty of Business and Communications, INTI International University, Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

2. Department of Management Studies, COEP, Technological University, Pune, India

3. Dibrugarh University, Assam, India

4. Nootan College of Nursing, Sankalchand Patel University, Visnagar, India

*Correspondence: asmatarakhan111@gmail.com

ABSTRACT

OBJECTIVE

The paper aims to examine ethical, privacy, and governance challenges in AI-IoT (Artificial Intelligence-based Internet of Things) healthcare environments.

DESIGN

A total of 39 peer-reviewed open-access studies were screened and used for a systematic review using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework. A multi-stage thematic analysis was used for identifying recurring patterns within the literature and answering the research questions.

RESULTS/OUTCOMES

The identified challenges in the AI-IoT healthcare ecosystems, arising from the thematic analysis, are privacy and continuous surveillance, algorithmic bias and lack of explainability, limitations for informed consent, and fragmented governance and accountability.

CONCLUSION

The findings, in sync with STS theory, indicate that challenges in AI-IoT healthcare systems cannot be addressed solely through technological innovations. In response, the study proposed an Integrated Human-Centric Trust Framework to integrate human intervention with technological advancements.

KEYWORDS

Internet of Things; Artificial Intelligence; Healthcare; Thematic Analysis; Law and Governance

INTRODUCTION

The healthcare industry is advancing due to continuous developments in digital technology, specifically Artificial Intelligence (AI) and the Internet of Things (IoT), creating smart healthcare networks that enable real-time tracking, predictive analysis, and customised medical treatment. IoT is benefitting the healthcare industry through increased innovation (80%), visibility across the organisation (76%), and cost savings (73%) through the use of devices, such as smart inhalers, connected medication dispensers, and wearable sensors [3]. Their applications lie in tracking vital signs and gathering large amounts of patient information for better diagnosis and treatment procedures. Even the introduction of the Internet of Medical Things (IoMT) in healthcare has led to uninterrupted communication between patients and healthcare providers. IoMT applications in portable diagnostic deliver patient care, allowing for remote care, disease prevention, and continuous patient monitoring, particularly for chronic disease patients and senior citizens [3]. However, the reliability of such technologies on a network makes them vulnerable to cyberattacks, creating privacy issues for personal information like identification and health status [4]. Also, continuous collection of large amounts of sensor data in healthcare settings might improve the quality of care but pose continuous ethical challenges in terms of data management, bias and fairness, and informed consent [5].

The continuous flow of data enabled by IoT technology creates an ecosystem of constant surveillance, raising concerns about patients' privacy [5]. In addition, the lack of transparency in medical AI development, also known as the 'black box' problem, raises concerns about trust, accountability, and fairness in healthcare services [6], [7]. This further reinforces the point of informed consent to understand why/how patient data is utilised by the governing bodies in AI-IoT-enabled healthcare [8]. Additionally, the conventional understanding of consent can no longer be applied to the healthcare system, given the constant flow of information enabled by IoT technology, which is reused for various purposes in healthcare settings [9], [10].

Taken together, there is a strong need for explainability in governance and opening the black box has become essential to provide a watershed moment unpacking ethical, privacy, and governance concerns, including trust in AI-based IoT healthcare. While existing literature has extensively discussed privacy, explainability, ethical AI, and governance concerns in healthcare technologies, these discussions remain fragmented across technical, legal, and ethical domains. This study contributes by providing an integrated thematic synthesis of interconnected challenges, thereby presenting an Integrated Conceptual Human-Centric Trust Framework that positions trust, accountability, patient autonomy, and governance as central dimensions of AI-IoT healthcare implementation. The two research questions are:

RQ1: What are the major ethical, privacy, and governance challenges associated with AI-IoT-enabled smart healthcare systems?

RQ2: How do ethical, privacy, and governance challenges within AI-IoT healthcare ecosystems influence patient trust, accountability, and human-centred healthcare delivery?

THEORETICAL LENS

The study is conceptually led by Socio-Technical Systems (STS) Theory, emphasising the interdependent relationships between technological systems and social, institutional, and human environments within the healthcare industry. In this study, STS guides the thematic exploration of governance, trust, explainability, and human-centred healthcare delivery.

LITERATURE REVIEW

AI and IoT technologies have combined to become a transformative area of development in healthcare today, as they provide effective patient care through improved clinical delivery and accurate diagnosis. Rushabh et al. [1] found increasing applications of AI and IoT technologies, including patient monitoring systems, disease detection, and wearable devices, further highlighting the need for system accuracy, security, data collection and management, and privacy protection to support their continued development. Wearable devices and IoT-based healthcare systems enable

individualised and remote care by providing continuous monitoring of multiple physiological parameters and facilitating early disease detection [11], [12]. AI-based healthcare models have demonstrated similar reliability in predicting patient health outcomes and supporting clinicians' decisions [13].

Smart healthcare ecosystems focus on the contributions of AI-based IoT systems to addressing societal and healthcare issues, such as population growth, resource scarcity, and the management of chronic health conditions [14]. Emerging technologies have created new paradigms in personalised healthcare; however, IoT devices and their data collection processes have been recognised as potential sources of data privacy and security breaches [15], [16]. Various studies have highlighted the need to ensure security by implementing security models such as encryption and blockchain [17], [18].

Furthermore, privacy is also at risk due to the widespread use of IoT monitoring systems that often operate without user consent or knowledge, challenging traditional healthcare models [8]. The integration of AI into these IoT monitoring systems raises further privacy concerns about algorithmic bias and fairness. Bias in the input data used to train the algorithms, and in the way algorithms are designed, means that individuals will receive inaccurate predictions and outcome measures, especially those belonging to disadvantaged populations [7], [19].

In response to these concerns, Explainable AI (XAI) has emerged as a useful way to provide transparency and show how AI processes clinical decisions [20], [21]. Clinicians who use XAI methods such as Shapley Additive Explanations (SHAP) and Local Interpretable Model Agnostic Explanations (LIME) have a better understanding of the model's output, in addition to trust in AI systems for patient treatment [22]. Another challenge in AI-IoT-based healthcare systems concerns informed consent. The traditional concept of consent is found to be inadequate in situations where data is constantly being created and reused [9]. New concepts such as dynamic consent and blockchain technology are proposed to address this challenge and provide users with better control and transparency in data usage [23]. Research highlights the importance of integrated governance and trustworthy AI models in the context of healthcare systems based on AI [24, 25]. The challenges with AI-IoT systems in terms of ethics are not only issues of technological limitations but rather of governance concerns that involve patient autonomy, compliance, accountability, and the overall trust in healthcare delivery, by combining the points from the literature. Finally, patient trust and acceptability are essential for AI-based healthcare systems. Research has shown that although patients acknowledge the benefits of AI-enabled health care systems, they are apprehensive about the consequences of losing personal data, personal autonomy and human interaction in the decision-making process [26].

RESEARCH GAPS

Existing research studies have proposed XAI privacy-preserving technologies and dynamic consent models as effective solutions. Their relevance and implementation within healthcare have not been fully developed. Available studies provide a limited understanding of the combined impact of these ethical and governance issues on accountability, trust and the overall quality of healthcare delivery.

METHODS

RESEARCH DESIGN

The study focuses on understanding AI and IoT-based ethical, privacy, and governance issues in healthcare, interrelating these constructs subjectively (guided by STS theory) and qualitatively (through a Systematic Literature Review).

SEARCH STRATEGY

A literature search was conducted using various databases, including Scopus, Springer, ScienceDirect, IEEE Xplore, and PubMed. These databases were considered for their broad coverage of interdisciplinary research involving healthcare technology applications, ethical AI, the IoT, and digital governance.

The search strategy employed Boolean operators and carefully selected keyword combinations to identify relevant scholarly literature related to Artificial Intelligence (AI), the Internet of Things (IoT), and healthcare ethics. Boolean operators such as “AND” were used to refine and narrow the search results by combining multiple concepts. The search string was:

((“Artificial Intelligence” OR AI) AND (“Internet of Things” OR IoT OR “Internet of Medical Things” OR IoMT) AND (Healthcare OR “smart healthcare” OR “digital healthcare”)) AND (“healthcare ethics” OR “ethical issues” OR “ethical challenges” OR “AI governance in healthcare” OR “Explainable AI” OR XAI OR “healthcare data privacy” OR “data protection” OR “algorithmic bias in healthcare AI” OR “informed consent in AI healthcare systems”))

These combinations enabled the identification of studies focusing on technological integration, ethical challenges, governance frameworks, transparency, privacy concerns, bias in AI-driven decision-making, and patient consent within intelligent healthcare environments.

INCLUSION CRITERIA

- English-language publications
- Literature focusing on AI, IoT, IoMT, machine learning, or explainable AI in healthcare contexts
- Peer-reviewed journal articles, conference proceedings, and scholarly book chapters discussing ethical, legal, governance, privacy, transparency, consent, or accountability dimensions
- Studies published between 2017 and 2025

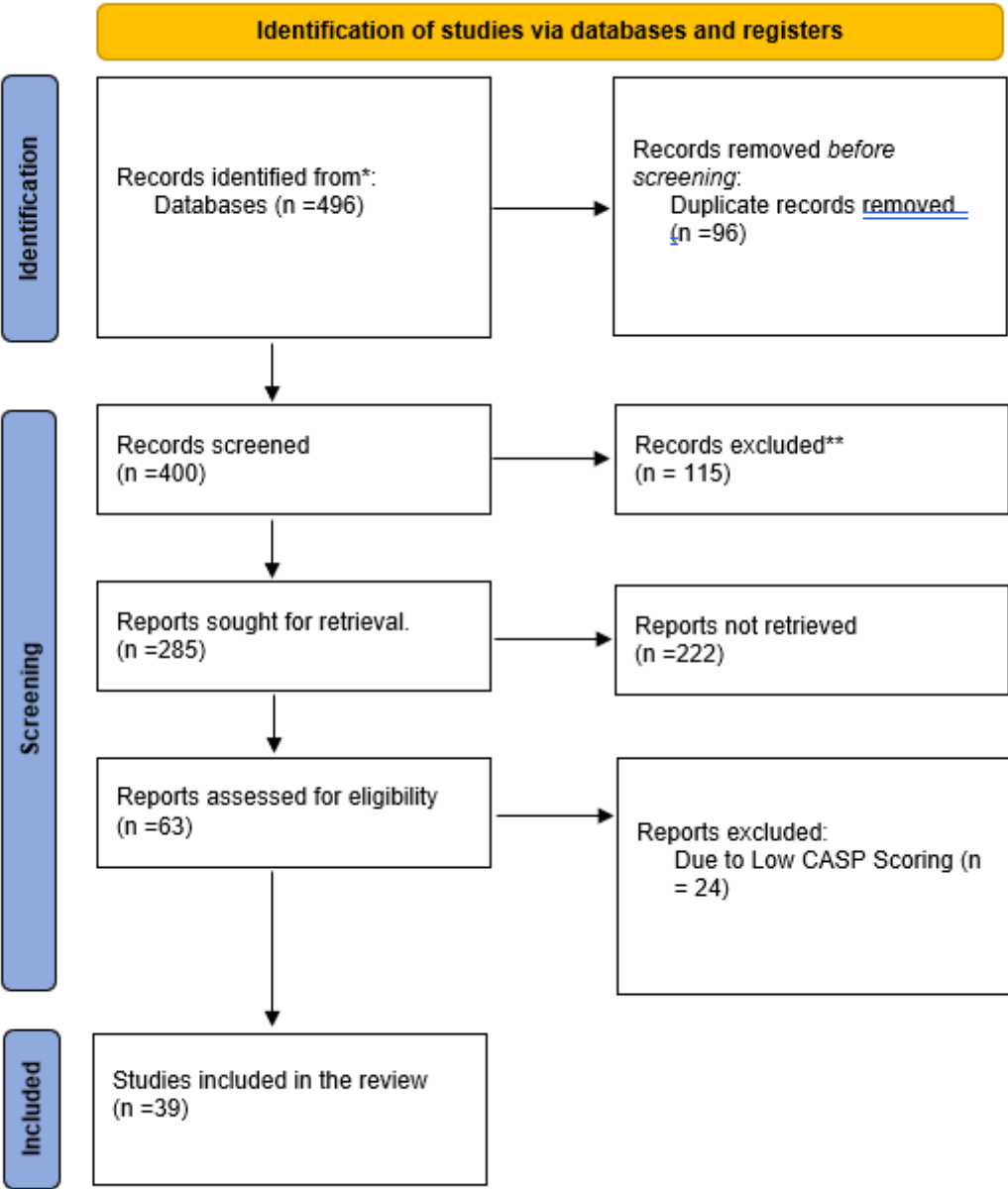
EXCLUSION CRITERIA

- Studies unrelated to healthcare applications
- Purely technical engineering studies without ethical or governance implications
- Non-peer-reviewed sources, editorials, blogs, or news reports
- Duplicate studies across databases
- Articles lacking an accessible full text

STUDY SELECTION PROCESS

Based upon the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework (Figure 1), the initial search was started using the Boolean search strings. The initial search yielded 496 articles for the contemporary period. Upon screening, it was found that out of 496 articles, 96 articles were duplicates and were thus removed. Moving forward, the 96 articles were further screened on the basis of inclusion and exclusion criteria. This resulted in the removal of 115 studies. The remaining 285 studies were then sought for report retrieval. Only 63 studies were retrieved. These 63 studies were then assessed on the basis of CASP (Critical Appraisal Skills Programme). Lastly, 39 studies were selected for the systematic literature review (Table 2).

FIGURE 1. PRISMA FLOWCHART



Source: Constructed by Authors

QUALITY APPRAISAL

The CASP framework provided a means to ensure the methodological quality and credibility of included studies by assessing them against common criteria, including: clearly defined study objectives, adequate methodological rigour, apparent validity of findings, relevance of findings to the research problem, ethical considerations, and transparency of analysis.

THEMATIC ANALYSIS

A multi-stage coding process was followed to ensure thematic consistency and analytical transparency. During the initial open coding stage, recurring concepts such as surveillance, explainability, bias, accountability, and governance were identified in the literature. In the second stage, these descriptive codes were grouped through axial coding into conceptual categories, i.e., ethics, privacy, and governance (Table 1). Finally, refinement was conducted using selective coding to categorise codes into analytical themes, which formed the foundation of this research's thematic interpretation.

TABLE 1. THEMATIC CODING AND CATEGORISATION

Category	Codes	Themes	Description
Privacy	privacy, surveillance, consent, data misuse, continuous monitoring	Theme 1 (RQ1)	Focuses on the protection of patient data, confidentiality, continuous IoT monitoring, informed consent practices, and risks associated with unauthorised access or secondary use of healthcare data.
Ethics	bias, explainability, transparency, trust, fairness, autonomy, human-centred care	Theme 2 (RQ1)	Covers ethical implications of AI-driven healthcare systems, including algorithmic bias, black-box AI, fairness in healthcare outcomes, transparency of decision-making, patient autonomy, and trust in AI systems.
Governance	governance, accountability, regulation, compliance, ethical oversight, liability	Theme 3 (RQ1)	Relates to regulatory frameworks, accountability mechanisms, AI governance structures, legal responsibility, policy compliance (e.g., GDPR), and institutional oversight of AI-IoT healthcare systems.

Source: Compiled by Authors

TABLE 2. SUMMARISATION OF LITERATURE

Year	Study Focus/Objective	Methodology/Approach	Key Findings	Codes	Themes	CASP Appraisal
[1]	AI and IoT integration in healthcare	Systematic literature review	AI-IoT improves monitoring and diagnostics	surveillance, governance	Governance	High
[2]	AI-IoT Healthcare 4.0 monitoring	Conceptual framework	Real-time predictive healthcare enhanced	surveillance, governance	Governance	Moderate
[3]	IoMT, AI, ML and smart healthcare future	Conceptual review	Smart technologies improve healthcare efficiency	surveillance, governance	Governance	Moderate
[4]	AI-enabled wearable IoT systems	Survey study	Wearables support continuous monitoring	surveillance, privacy	Privacy	High

[5]	Ethical issues in ambient intelligence healthcare	Ethical review	Surveillance threatens autonomy and privacy	privacy, surveillance, consent	Privacy	High
[6]	Explainability in healthcare AI	Multidisciplinary review	XAI improves transparency and trust	explainability, transparency	Ethics	High
[7]	Privacy challenges in AI healthcare	Literature review	Patients fear misuse of health data	privacy, accountability	Privacy	High
[8]	Privacy-by-design in smart healthcare	Conceptual analysis	Existing consent systems are inadequate	consent, governance	Privacy	High
[9]	AI, big data and consent	Theoretical analysis	Traditional consent models fail in AI systems	consent, accountability	Ethics	High
[10]	Legal and ethical concerns in healthcare AI	Review study	Responsibility for AI decisions remains unclear	accountability, governance	Governance	High
[11]	ML for healthcare wearables	Technical review	ML improves predictive monitoring	surveillance	Governance	Moderate
[12]	AI-IoT for critical healthcare	Applied review	AI enables real-time healthcare response	surveillance, accountability	Governance	Moderate
[13]	Secure wearable healthcare systems	CPS and IoT review	Security essential for healthcare trust	Privacy, governance	Privacy	Moderate
[14]	IoT and ML in smart healthcare	Review article	Predictive AI supports healthcare efficiency	Surveillance/governance	Governance	Moderate

[15]	ML for healthcare-IoT security	Risk mitigation review	IoT vulnerabilities threaten healthcare systems	Accountability, governance	Governance	High
[16]	Data privacy in AI healthcare	Narrative review	AI challenges healthcare privacy norms	Privacy/surveillance	Privacy	Moderate
[17]	Secure IoT healthcare systems	Conceptual review	Secure architecture improves trust	governance	Governance	Moderate
[18]	ML anomaly detection in healthcare IoT	Experimental study	ML enhances security monitoring	Surveillance/governance	Governance	High
[19]	IoT and ML for personalized healthcare	Conference study	Personalized care faces interoperability challenges	Accountability/governance	Governance	Moderate
[20]	Explainable AI diagnostics	Conceptual analysis	XAI improves accountability	Explainability/accountability	Ethics	Moderate
[21]	XAI and healthcare trust	Review study	Transparency strengthens trust	explainability, transparency, trust	Ethics	High
[22]	XAI and ethical compliance	Conceptual review	Ethical AI requires transparency	explainability, governance, accountability	Ethics	Moderate
[23]	Blockchain-based dynamic consent	Technological framework	Dynamic consent improves patient control	consent, privacy	Privacy	High

[24]	Trustworthy AI in healthcare	Ethical review	Governance pathways are essential	governance, accountability	Governance	High
[25]	AI governance framework in healthcare	Multimethod protocol	Governance frameworks support safe AI adoption	governance, accountability	Governance	High
[26]	Public perception of healthcare AI	Survey study	Public expresses privacy and ethical concerns	privacy, trust, consent	Ethics	High
[27]	Ethical conundrums in AI healthcare	Scoping review	AI raises fairness and accountability concerns	bias, accountability, governance	Ethics	High
[28]	AI ethics under GDPR	Comprehensive review	GDPR stresses transparency obligations	governance, privacy, accountability	Governance	High
[29]	Security and privacy in IoT healthcare	Review article	Smart healthcare vulnerable to cyber threats	privacy, surveillance	Privacy	High
[30]	IoT communication security in healthcare	Technical review	Security mechanisms strengthen privacy	privacy, governance	Privacy	Moderate
[31]	Big data and predictive analytics	Perspective article	Predictive analytics may threaten patient interests	privacy, accountability, trust	Ethics	High
[32]	XAI with ML for disease prediction	Empirical review	Explainability improves trust and transparency	explainability, transparency	Ethics	High

[33]	Actionable ethics in digital health	Ethical framework analysis	Ethical oversight should be operationalized	governance, accountability, consent	Governance	High
[34]	AI ethics and managerial foresight	Conceptual review	Ethical imperatives shape sustainable healthcare	governance, accountability	Governance	Moderate
[35]	Safe and trustworthy AI systems	Review article	Trustworthy AI requires accountability and ethics	governance, accountability, trust	Governance	High
[36]	AI, IoT and wearable healthcare	Book chapter review	Emerging technologies improve diagnostics	surveillance, governance	Governance	Moderate
[37]	AI for IoT medical systems	Conceptual chapter	AI enhances intelligent healthcare systems	governance, surveillance	Governance	Moderate
[38]	Health Industry 4.0,5.0 trends	Bibliometric analysis	AI-healthcare research rapidly expanding	governance	Governance	Moderate
[39]	Digital healthcare disease prediction	Review study	Predictive systems improve diagnosis	surveillance, accountability	Governance	Moderate

Source: Constructed by Authors

ANALYSIS AND RESULTS

THEME 1. PRIVACY AND CONTINUOUS DATA SURVEILLANCE (RQ1)

Theme 1 aligns with patients' private information, including physiological data, behavioural patterns, and lifestyle details being collected through AI-IoT devices. Cyberattacks and vulnerabilities in connected networks directly or indirectly challenge data surveillance, increasing risks of breaches, illegal access, and misuse. The use of centralised data storage, together with cloud computing services, further exacerbates risks because both storage systems and communication protocols have security weaknesses. The process of collecting data without notifying users results in patients experiencing invisible data extraction. The situation creates an unequal distribution of power between patients and healthcare providers, resulting in privacy issues. Moreover, the reuse of data for secondary purposes, such as research, data analysis, or business, has increased the complexity of informed consent.

THEME 2. ALGORITHMIC BIAS AND LACK OF EXPLAINABILITY (RQ1)

Ethical challenges of AI-IoT systems are a lack of explainability and algorithmic bias that can arise for many reasons, including imbalanced datasets, lack of validation and weakness in governance measures during deployment. Biases shape and drive the unequal experiences of health care and significantly impact underrepresented patient populations. Additionally, the lack of understanding of AI-generated recommendations (in some cases) results in the black box property of AI systems and transparency issues. XAI could be a potential solution to increase transparency in the healthcare system, but it has to be paired with continuous ethical oversight and organisational accountability/prejudice checks. STS Theory suggests that these moral dilemmas should be approached not merely as a technical problem, but as a consequence of the closed relationships between technology, governance, healthcare organisations, and human decision-making.

THEME 3. GOVERNANCE, REGULATION, AND ACCOUNTABILITY GAPS (RQ1)

Theme 3 reflects the fact that AI-IoT systems deployed in health care settings are often subjected to governance and accountability issues. When the current regulatory and institutional frameworks don't evolve as quickly as AI technologies, the issues escalate into problems of patient safety, transparency, and institutional accountability. Rather, these governance issues, in the STS perspective, are not exclusively caused by the technological innovation itself, but by the complex interplay of factors, including AI systems, regulatory frameworks, healthcare contexts, and human decision-making processes. Only an integrated governance approach can help address these issues and enhance transparency, compliance, patient trust and human-centred care.

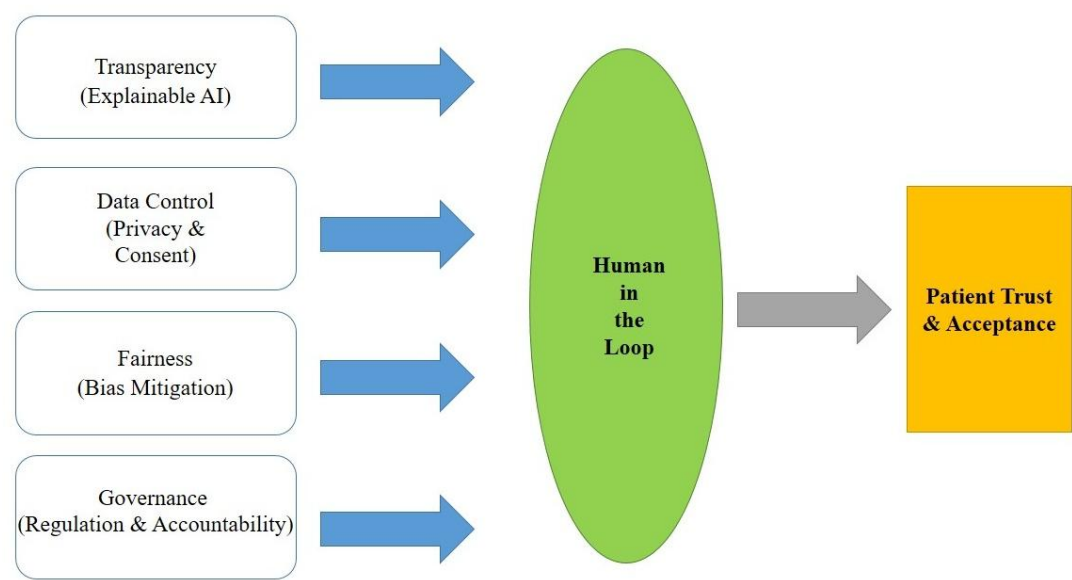
TRUST, ACCOUNTABILITY, HUMAN-CENTRED HEALTHCARE DELIVERY (RQ2)

Thematic analysis collectively reveals that lack of trust in AI-IoT-based healthcare systems exists because of issues with surveillance, biased algorithmic methods and governance. Concerns about privacy introduced problems relating to autonomy and informed consent, and institutional control of patient data. Similarly, the opacity of AI also posed challenges to operational processes, impacting the accountability of healthcare professionals for patient outcomes. Moreover, roles to be held accountable are not clearly specified, leaving room for doubts about ethical responsibility, particularly in the case of wrong diagnosis or prognosis and adverse clinical results. All these factors significantly affect transparency, compliance and public confidence in AI-supported healthcare delivery. The research, therefore, suggests that accountability in AI-IoT systems is not merely a technical issue but also an institutional governance challenge (STS perspective). In this context, the Integrated Conceptual Human-Centric Trust Framework emerges as a socio-technical governance approach, aiming to strengthen ethical AI implementation, institutional trust, and patient-centred healthcare delivery in digitised healthcare environments.

The Integrated Conceptual Human-Centric Trust Framework, as shown in Figure 2, builds a foundation for digital healthcare by outlining four fundamental elements of trust and how they impact transparency, patient control of data, fairness, and governance. Transparency supports clinical confidence because it enables stakeholders to make effective decisions using AI-IoT-supported systems. Patient control over data emphasises informed consent, privacy protection, and meaningful control over personal healthcare information. Fairness addresses the ethical risks of unequal healthcare outcomes caused by opaque AI decision-making processes. Governance functions as the foundational mechanism that supports institutional accountability, compliance and responsible AI deployment. At the centre of the frameworks is the Human-in-the-loop approach, suggesting that continued involvement of healthcare professionals is necessary in validating AI-supported decisions. From the STS perspective, it means that trustworthy healthcare requires a fine balance between technological innovations, human interventions, institutional accountability, patient-centred healthcare approaches and ethical oversight.

This holistic framework combines patient autonomy, fairness, governance and human oversight, unlike current frameworks which tend to focus on one or the other or on technical transparency in isolation. It makes trust a governance and management issue, rather than a technical matter. Nevertheless, the framework is still conceptual and needs to be validated in various healthcare environments for its practical application and operational effectiveness.

FIGURE 2. HUMAN CENTRIC TRUST FRAMEWORK FOR IOT ENABLED SMART HEALTHCARE SYSTEMS



Source: Constructed by Authors

Whereas, given the current state of frameworks and literature, such as WHO Ethical guidelines, trustworthy AI models, and GPR principles, there is a lack of unified socio-technical perspectives, particularly with concepts of patient autonomy, transparency and fairness in place as well as governance and human oversight (Table 3).

TABLE 3. COMPARISON BETWEEN EXISTING FRAMEWORKS

Existing Frameworks	Primary Focus	Limitation	Contribution of the Proposed Framework
WHO Ethical AI Guidance	Ethical AI principles	Broad healthcare ethics orientation	Integrates governance and trust within AI-IoT healthcare ecosystems
GDPR Principles [28]	Data privacy and compliance	Focused mainly on data governance	Incorporates institutional accountability and human oversight
Trustworthy AI Frameworks [35]	Transparency and fairness	Limited healthcare operational focus	Contextualises trust within healthcare delivery systems
Healthcare Governance Models [25]	Institutional accountability	Limited AI-IoT integration	Synthesises governance, ethics, and socio-technical trust dimensions

Source: Compiled by Authors from [25, 26, 35]

LIMITATIONS AND CONCLUSIONS

Some of the limitations of this research are as follows:

- The study relies on secondary literature and thematic analysis, which may introduce some subjectivity and bias in identifying and interpreting themes.
- The small sample of 39 studies may not fully capture the rapidly evolving nature of AI-IoT technology.
- The proposed framework is conceptual and is not empirically validated.

These limitations call for future empirical studies to validate the findings and enhance the practical implementation and operational efficacy of the proposed framework. Given these findings, continued research is needed to fully grasp the intricate interplay between healthcare facilities, AI systems, governance, and human decision-making processes, and

shift the norms and expectations of AI use. Further studies are necessary to build a balance between technological advancements and human interventions.

References

1. Shah R, Chircu A. IoT and AI in Healthcare: A Systematic Literature Review. *Issues Inf Syst* 2018; 19(3):33-41. https://doi.org/10.48009/3_iis_2018_33-41
2. Kishor A, Chakraborty C. Artificial intelligence and Internet of Things-Based Healthcare 4.0 Monitoring System. *Wirel Pers Commun* 2022; 127(2):1615-31. <https://doi.org/10.1007/s11277-021-08708-5>
3. Venkatesh DA. Reimagining the Future of Healthcare Industry through Internet of Medical Things (IoMT), Artificial Intelligence (AI), Machine Learning (ML), Big Data, Mobile Apps and Advanced Sensors. *Int J Eng Adv* 2019; 9(1). <https://www.ijeat.org/wp-content/uploads/papers/v9i1/A1412109119.pdf>
4. Subhan F et al. AI-enabled Wearable Medical Internet of Things in Healthcare System: A Survey. *Appl Sci* 2023; 13(3):1394. <https://doi.org/10.3390/app13031394>
5. Martinez-Martin N et al. Ethical issues in using ambient intelligence in Health-Care Settings. *Lancet Digit Health* 2021; 3(2):e115-23. [https://doi.org/10.1016/S2589-7500\(20\)30275-2](https://doi.org/10.1016/S2589-7500(20)30275-2)
6. Amann J, Blasimme A, Vayena E, Frey D, Madai VI, Precise4Q Consortium. Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective. *BMC Med Inform Decis Mak* 2020; 20(1):310. <https://doi.org/10.1186/s12911-020-01332-6>
7. Williamson SM, Prybutok V. Balancing privacy and progress: a review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-driven Healthcare. *Appl Sci*. 2024; 14(2):675. <https://doi.org/10.3390/app14020675>
8. O'Connor Y, Rowan W, Lynch L, Heavin C. Privacy by design: Informed Consent and Internet of Things for Smart Health. *Procedia Comput Sci* 2017; 113:653-8. <https://doi.org/10.1016/j.procs.2017.08.329>
9. Andreotta AJ, Kirkham N, Rizzi M. AI, Big Data, and the Future of Consent. *AI & Society*. 2022; 37(4):1715-28. <https://doi.org/10.1007/s00146-021-01262-5>
10. Naik N et al. Legal and Ethical Considerations in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Front Surg* 2022; 9:862322. <https://doi.org/10.3389/fsurg.2022.862322>
11. Sabry F, Eltaras T, Labda W, Alzoubi K, Malluhi Q. Machine Learning for Healthcare Wearable Devices: The Big Picture. *J Healthc Eng* 2022; 2022(1):4653923. <https://doi.org/10.1155/2022/4653923>
12. Shumba AT, Montanaro T, Sergi I, Fachechi L, De Vittorio M, Patrono L. Leveraging IoT-aware Technologies and AI Techniques for Real-time Critical Healthcare Applications. *Sensors* 2022; 22(19):7675. <https://doi.org/10.3390/s22197675>
13. Ramasamy LK, Khan F, Shah M, Prasad BV, Iwendi C, Biamba C. Secure Smart Wearable Computing through Artificial Intelligence-enabled Internet of Things and Cyber-Physical Systems for Health Monitoring. *Sensors* 2022; 22(3):1076. <https://doi.org/10.3390/s22031076>
14. Ghazal TM et al. IoT for smart cities: Machine learning approaches in Smart Healthcare—A Review. *Future Internet* 2021; 13(8):218. <https://doi.org/10.3390/fi13080218>
15. Khatun MA, Memon SF, Eising C, Dhirani LL. Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. *IEEE Access*. 2023; 11:145869-96. <https://doi.org/10.1109/ACCESS.2023.3346320>
16. Yadav N, Pandey S, Gupta A, Dudani P, Gupta S, Rangarajan K. Data Privacy in Healthcare: In the Era of Artificial Intelligence. *Indian Dermatol Online J* 2023; 14(6):788-92. https://doi.org/10.4103/idoj.idoj_543_23
17. Panahi O. Secure IoT for Healthcare. *EJSS* 2025; 1(1):17-23. [https://doi.org/10.59324/ejss.2025.1\(1\).03](https://doi.org/10.59324/ejss.2025.1(1).03)
18. Khan MM, Alkathami M. Anomaly detection in IoT-based healthcare: Machine Learning for Enhanced Security. *Sci Rep* 2024; 14(1):5872. <https://doi.org/10.1038/s41598-024-56126-x>
19. Ahamed F, Farid F. Applying Internet of Things and Machine Learning for Personalised Healthcare: Issues and Challenges. In: *Proceedings of ICMLDE*; 2018; 19-21. <https://ieeexplore.ieee.org/document/8613997>
20. Akande OA. Leveraging Explainable AI Models to Improve Predictive Accuracy and Ethical Accountability in Healthcare Diagnostic Decision Support Systems. *World J Adv Res Rev* 2020; 8(2):415-34. <https://doi.org/10.30574/wjarr.2020.8.2.0384>
21. Adeniran AA, Onebunne AP, William P. Explainable AI (XAI) in Healthcare: Enhancing Trust and Transparency in Critical Decision-Making. *World J Adv Res Rev* 2024; 23(3):2647-58. <https://doi.org/10.30574/wjarr.2024.23.3.2936>

22. Daram S. Explainable AI in healthcare: Enhancing trust, transparency, and Ethical Compliance in Medical AI Systems. *IJAIBDCMS* 2025; 6(2):11-20. <https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I2P102>
23. Albanese G, Calbimonte JP, Schumacher M, Calvaresi D. Dynamic Consent Management for Clinical Trials via Private Blockchain Technology. *J Ambient Intell Humaniz Comput* 2020; 11(11):4909-26. <https://doi.org/10.1007/s12652-020-01761-1>
24. Goktas P, Grzybowski A. Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI. *J Clin Med* 2025; 14(5):1605. <https://doi.org/10.3390/jcm14051605>
25. Freeman S et al. Developing an AI Governance Framework for Safe and Responsible AI in Health Care Organizations: Protocol for a Multimethod Study. *JMIR Res Protoc* 2025; 14(1):e75702. <https://doi.org/10.2196/75702>
26. Witkowski K, Dougherty RB, Neely SR. Public Perceptions of Artificial Intelligence in Healthcare: Ethical Concerns and Opportunities for Patient-Centered Care. *BMC Medical Ethics* 2024; 25(1):74. <https://doi.org/10.1186/s12910-024-01066-4>
27. Prakash S, Balaji JN, Joshi A, Surapaneni KM. Ethical conundrums in the Application of Artificial Intelligence (AI) in Healthcare—A Scoping Review of Reviews. *J Pers Med* 2022; 12(11):1914. <https://doi.org/10.3390/jpm12111914>
28. Mohammad AM, Jesus M, Fanaei SD, Alves P, Hassanzadeh BA, Hariri F. Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate. *Mach Learn Knowl Extr* 2023; 5(3):1023-35. <https://doi.org/10.3390/make5030053>
29. Karunarathne SM, Saxena N, Khan MK. Security and Privacy in IoT Smart Healthcare. *IEEE Internet* 2021; 25(4):37-48. <https://doi.org/10.1109/MIC.2021.3051675>
30. Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. *Sensors* 2023; 23(21):8944. <https://doi.org/10.3390/s23218944>
31. Balthazar P, Harri P, Prater A, Safdar NM. Protecting Your Patients' Interests in the Era of Big Data, Artificial Intelligence, and Predictive Analytics. *J Am Coll Radiol* 2018; 15(3):580-6. <https://doi.org/10.1016/j.jacr.2017.11.035>
32. Agrawal R, Gupta T, Gupta S, Chauhan S, Patel P, Hamdare S. Fostering Trust and Interpretability: Integrating Explainable AI (XAI) with Machine Learning for Enhanced Disease Prediction and Decision Transparency. *Diagn Pathol* 2025; 20(1):105. <https://doi.org/10.1186/s13000-025-01686-3>
33. Nebeker C, Torous J, Bartlett Ellis RJ. Building the Case for Actionable Ethics in Digital Health Research Supported by Artificial Intelligence. *BMC Med* 2019; 17(1):137. <https://doi.org/10.1186/s12916-019-1377-7>
34. Sodhi SK, Bansal S, Saxena U. Artificial Intelligence in Healthcare: Market Dynamics, Ethical Imperatives, and Managerial Foresight. *Prabandhan: Indian Journal of Management* 2025; 15:79-84. <https://doi.org/10.17010/pijom/2025/v18i9/174845>
35. Jenko S et al. Artificial Intelligence in Healthcare: How to Develop and Implement Safe, Ethical and Trustworthy AI Systems. *AI*. 2025; 6(6):116. <https://doi.org/10.3390/ai6060116>
36. Banerjee A, Chakraborty C, Rath S. Medical Imaging, Artificial Intelligence, Internet of Things, Wearable Devices in Terahertz Healthcare Technologies. In: *Terahertz Biomedical and Healthcare Technologies* 2020; 145-165. <https://doi.org/10.1016/B978-0-12-818556-8.00008-2>
37. Oniani S, Marques G, Barnovi S, Pires IM, Bhoi AK. Artificial Intelligence for Internet of Things and Enhanced Medical Systems. In *Bio-inspired Neurocomputing* 2020; 43-59. https://doi.org/10.1007/978-981-15-5495-7_3
38. Dany YA, Pribadi F. Trends of Research in Hospital Financing and Health Industry 4.0,5.0: A Bibliometric Analysis. *Asia Pac J Health Manag* 2025; 20(1):385-94. <https://doi.org/10.24083/apjhm.v20i1.3695>
39. Garg J, Singh AK. The Use of Digital Healthcare Systems to Predict Diseases. *Asia Pac J Health Manag* 2023; 18(1):267-74. <https://doi.org/10.24083/apjhm.v18i1.1679>