Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Internet of Things in Healthcare: Applications, Challenges, and Future Directions

Almohairie A. Bantas
Department of Computer Engineering
University of Southern Mindanao
Kabacan, Cotabato, Philippines

John Lawrence R. Tobias
Department of Computer Engineering
University of Southern Mindanao
Kabacan, Cotabato, Philippines

Vhon Bryan B. Silvano
Department of Computer Engineering
University of Southern Mindanao Kabacan,
Cotabato, Philippines

Abstract **-** Despite rapid advances in Internet of Things (IoT) technologies for healthcare, existing studies remain fragmented—focusing separately on technical development, security, or clinical applications without an integrated view of practical barriers. This systematic review of 15 peer-reviewed articles (2015–2025) follows PRISMA guidelines to synthesize evidence on IoT applications, challenges, and future directions. The analysis identifies three primary application domains: remote patient monitoring, smart healthcare management, and telemedicine. While these domains offer significant benefits, their real-world effectiveness is consistently undermined by interoperability gaps, security vulnerabilities, and unresolved ethical and regulatory issues. This review contributes an integrated analytical framework that links technological capabilities with persistent implementation barriers, revealing critical gaps in scalability, regulatory alignment, and long-term sustainability. It concludes that future research must move beyond isolated innovations toward standardized, ethically grounded, and scalable IoT architectures to realize safe and equitable digital healthcare.

Keywords – Internet of Things, IoT, Healthcare, remote patient monitoring, Challenges, Future Directions

I. INTRODUCTION

The Internet of Things (IoT), that connects hardware, sensors, and software online, has progressively altered how systems function. This capability has progressively altered how systems function, including in healthcare. IoT allows real-time monitoring of patients through wearable technology, implantable sensors, and smart medical equipment [3], [8]. These devices can monitor vital signs such as blood pressure, heart rate, and oxygen saturation, and transmit the data instantaneously to medical professionals [3], [5]. IoT is also used in hospitals to track medical equipment, manage inventories, monitor environmental factors like temperature and air quality, and improve operational efficiency [11], [13].

During the COVID-19 pandemic, IoT became even more crucial. It enabled remote patient monitoring and reduced unnecessary hospital stays, while allowing healthcare workers to maintain social distancing [3]. Patients can now receive ongoing care at home rather than relying solely on scheduled clinic visits. This shift supports preventative healthcare, where continuous data collection enables early detection of health issues [5], [8]. Additionally, patient engagement increases when individuals can access their own health data [3].

However, the widespread adoption of IoT in healthcare also introduces significant challenges. Sensitive patient data becomes prone to privacy risks and potential exploitation [15]. Technical issues include the growing number of sensors, increased processing demands, energy consumption, and data quality loss during transmission [4]. Furthermore, healthcare systems must comply with strict privacy regulations such as HIPAA and GDPR, which can be costly and complex, especially when IoT data is processed in cloud environments or transported across borders [2], [12]. Ethical obligations regarding patient data, telemonitoring, and the use of IoT in clinical decision-making must also be carefully considered [14].

Integrating IoT into healthcare requires more than adding gadgets. It necessitates changing how information flows, storing and analyzing sensor data to support precise medical decisions, and ensuring secure data management and reliable networks. Even the most sophisticated devices will not improve outcomes unless they are properly integrated into clinical workflows [4], [11]. Therefore, studying IoT in healthcare entails looking beyond the technology itself to examine how it fits into real clinical settings and routine medical practices [13].

Emerging technologies offer potential solutions. Artificial intelligence can process massive IoT datasets, with applications in diagnosis, disease prediction, and clinical decision-making [1], [9]. Privacy-enhancing technologies (PETs) can reduce privacy risks and safeguard personally identifiable information [6]. Edge and fog computing enable scalable and responsive IoT networks by shifting processing and storage from

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

centralized cloud servers to the network edge, supporting large-scale healthcare applications [7],[10].

Understanding these opportunities, along with the persistent challenges, is crucial as healthcare systems become increasingly digital. A better understanding of these factors can help ensure that IoT systems are not only innovative but also safe, reliable, and sustainable [14], [15].

Despite the growing body of research, current studies frequently treat IoT applications in distinct silos, some focus on monitoring systems and wearables, others on artificial intelligence or security issues leaving a gap in organized discussions that link applications, practical difficulties, and emerging technologies. Moreover, while many academics emphasize the promise of IoT, fewer studies examine real-world issues such as long-term sustainability, infrastructural constraints, data privacy hazards, and regulatory compliance. This fragmented conversation calls for a targeted synthesis that unifies these components.

Based on the existing literature, four significant gaps remain: (1) a lack of studies combining applications, challenges, and emerging technologies into a single analytical framework; (2) limited attention to ethical obligations and practical regulatory compliance; (3) insufficient discussion of how AI, edge computing, and privacy technologies can be sustainably integrated; and (4) understudied implementation barriers such as interoperability, cost, and infrastructure preparedness across diverse healthcare settings

This study addresses these gaps by conducting a structured systematic review of IoT in modern healthcare systems. It seeks to answer four research questions: What are the primary applications of IoT in healthcare? What recurring technological, ethical, and regulatory challenges impede adoption? What critical security and privacy concerns exist? What promising future directions involve AI, edge computing, and privacy-enhancing technologies? The review is significant for researchers, healthcare organizations, policymakers, and system developers, as it provides an analytical overview of the field, practical insights into benefits and constraints, and guidance for embedding security and interoperability into future designs. The scope is limited to peer-reviewed literature from 2015 to 2025 focusing on wearable technology, smart hospitals, patient monitoring, remote healthcare services, and integration with emerging technologies; it excludes experimental system development and detailed hardware-level engineering.

II. Review of Related Literature

Three main areas of IoT use in healthcare are revealed by the analysis of the 15 reviewed papers. These areas are related, but they have different traits and difficulties.

A. Remote Patient Monitoring

Remote patient monitoring (RPM) is the most extensively documented IoT application in healthcare [3], [5], [11]. RPM uses wearable technology, implantable sensors, and intelligent monitoring systems to continuously track vital physiological parameters such as heart rate, blood pressure, glucose levels, and oxygen saturation [3], [8], [14]. Dian et al. [8] describe how wearables can be attached to the skin, integrated into clothing, or implanted, communicating seamlessly with smartphones to gather and transmit health data. Al-Kahtani et al. [3] emphasize that the clinical value of RPM lies not only in data collection but in its integration into workflows for proactive intervention—an observation that carries analytical weight: without workflow alignment, data collection becomes an end rather than a clinical tool.

During the COVID-19 pandemic, RPM enabled remote patient management, reducing viral transmission while maintaining care quality [3], [13]. Analytically, this context was decisive: the pandemic created both an urgent need and a temporary relaxation of regulatory barriers, suggesting that RPM adoption is often crisis-driven rather than systematically planned. However, the literature also warns of data overload and the need for robust analytics, often involving artificial intelligence [1], [9], [14]. This points to a recurring tension: RPM generates continuous data streams, but most healthcare systems lack the analytical capacity to convert raw data into actionable insights. Ethical concerns regarding continuous monitoring and patient consent are further highlighted by Zakerabasali and Ayyoubzadeh [14]. Across all RPM studies, a consistent analytical finding emerges technological capability outpaces institutional readiness, creating a gap where data volume exceeds response capacity.

B. Smart Healthcare Management

Beyond direct patient care, IoT technologies are fundamentally reshaping hospital operations [2],[13]. This domain includes sensor-based tracking for inventory and equipment management, environmental monitoring, and workflow optimization [4], [7], [10], [12]. Espinosa et al. [13] note that RFID tags and sensor networks enable real-time asset tracking, reducing time spent searching for equipment and minimizing losses. Environmental monitoring in operating rooms and intensive care units ensures patient and staff safety by maintaining stable temperature, humidity, and air quality [13].

Smart healthcare management differs from RPM in its primary constraint: while RPM faces data overload, smart hospital systems face legacy integration barriers. Anmulwar et al. [4] and Alaba et al. [2] point out that integrating these systems within legacy hospital infrastructures poses significant interoperability challenges. This is not merely a technical nuisance—interoperability failure in smart hospitals that produce fragmented data environments where asset tracking, environmental monitoring, and patient records remain disconnected, undermining the promised efficiency gains. Regulatory compliance for such systems, especially concerning data handling, is addressed by Sahualla and Sahualla [12] and Zarkia and Usman [15]. Blockchain-based security solutions are explored by Khan et al. [10] as a potential way to enhance trust and data integrity. Critically, the literature suggests that trust and integrity are not automatically conferred by blockchain; they depend on standardization across heterogeneous devices, a precondition rarely met in practice.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

C. Telemedeecine and Emergency Response

The convergence of IoT and telemedicine has created powerful platforms for remote care, particularly in rural areas where access to specialists is limited [2], [3], [13]. IoT-enabled telemedicine systems allow physicians to access real-time vital signs during virtual consultations, improving remote diagnosis and chronic disease management [3], [5]. Ahmad et al. [1] and Karalis [9] discuss the role of artificial intelligence in analyzing telemedicine data to support clinical decision-making. In emergency scenarios, connected body-worn devices can monitor critical vitals and help target appropriate responses [3].

Telemedicine shares RPM's dependency on data quality but adds a real-time interaction requirement. However, the effectiveness of these systems depends on robust, low-latency network infrastructure, which may not be universally available [2], [4]. This introduces infrastructure heterogeneity as a mediating variable: in urban settings with reliable broadband, telemedicine can approximate in-person care; in rural or low-resource settings, latency and bandwidth limitations degrade service quality to the point of clinical risk. Ethical issues surrounding remote decision-making and the use of consumer-grade wearables are critically examined by Zakerabasali and Ayyoubzadeh [14] and Cha et al. [6]. Privacy-enhancing technologies, as reviewed by Cha et al. [6], offer promising solutions to protect patient data in telemedicine applications. Analytically, however, the literature lacks empirical evidence on whether PETs can operate effectively under low-latency emergency conditions gap that future research must address.

III. Methods and Procedures

This study employs a systematic review with an analytical synthesis orientation to examine how Internet of Things (IoT) technologies function within real healthcare systems, rather than merely cataloging their applications. The methodological focus is not only on identifying what has been studied, but on interrogating relationships between technological capabilities, implementation barriers, and clinical outcomes across the literature.

A systematic review design was selected because existing IoT healthcare research is highly fragmented, often isolating technical innovation, clinical application, or security concerns. This fragmentation limits understanding of how these components interact in practice. By applying a structured and comparative approach, this study aims to reconstruct a more integrated perspective, highlighting recurring constraints and causal patterns that influence real-world effectiveness.

A. Literature Seacrh Strategy

This study used four major academic databases—Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink—as key sources of literature to guarantee thorough and impartial coverage. A more comprehensive examination of IoT in healthcare is made possible by the unique viewpoints that each database offers, ranging from engineering-focused research to transdisciplinary and healthcare-oriented studies.

The search strategy employed Boolean operators to systematically combine keywords and capture both application-focused and challenge-oriented studies. The following search strings were used:

- "Internet of Things in Healthcare" OR "IoT in Healthcare"
- "IoT in Healthcare Applications" AND ("Wearable" OR "Remote Monitoring")
- "IoT Security in Healthcare" AND ("Privacy" OR "Data breach")
- "Challenges of IoT in Healthcare" AND ("Interoperability" OR "Regulation")
- "IoT Smart Healthcare Systems" AND ("AI" OR Edge Computing")

The literature search was conducted between February 26 and April 9, 2026. An iterative refinement process was applied, wherein search terms were adjusted based on emerging themes during preliminary screening to improve relevance without compromising methodological consistency.

B. Screening Process

A PRISMA framework guided the study selection process to ensure transparency, consistency, and reproducibility. Importantly, the screening process prioritized analytical relevance rather than volume, focusing on studies that contribute meaningful insights into IoT applications, challenges, and system-level implications.

- Inclusion Criteria

  1. Peer-reviewed articles, conference papers, and review papers published between January 2015 and December 2025.
  2. Studies focusing on IoT applications in wearable technology, smart hospitals, remote patient monitoring, and telemedicine.
  3. Studies that are available in full-text format and published in English to guarantee thorough analysis, uniformity, and accessibility.
  4. Articles that explicitly discussed applications, challenges, security, or future directions of IoT in healthcare.

- Exclusion criteria

  1. Articles focusing solely on hardware-level sensor engineering or experimental system development without broader healthcare application context.
  2. Non-peer-reviewed sources such as editorial, news articles, and white papers.
  3. Studies where IoT was a peripheral rather than a central theme.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

A systematic search of Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect yielded 120 records. After removing duplicates, 112 articles remained for title and abstract screening. Of these, 92 records were excluded because they focused on hardware-level engineering, were non-peer-reviewed, or did not address IoT in healthcare. The remaining 20 full-text articles were assessed for eligibility, of which 5 were excluded for not being in English or lacking relevance to the research questions. Consequently, 15 studies met all inclusion criteria and were included in the qualitative synthesis.

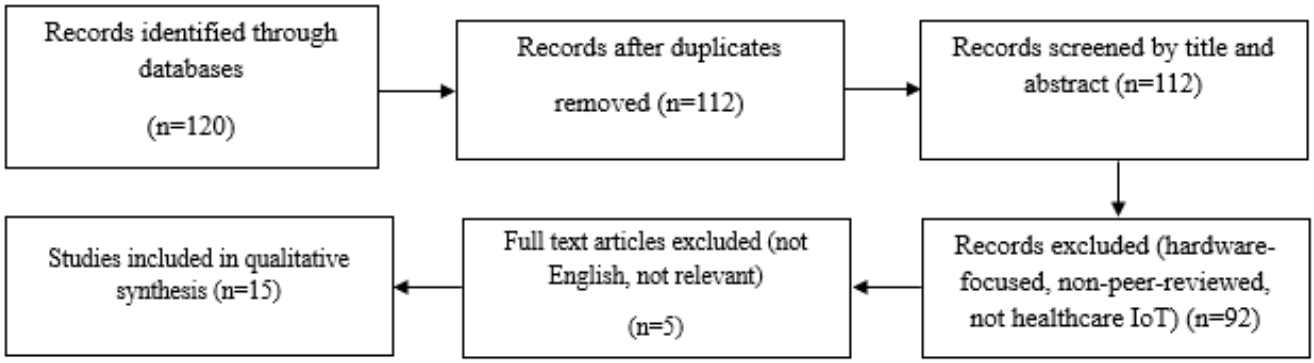

Figure 1: PRISMA Flow Diagram of Study Selection across four databases (Google Scholar, IEEE Xplore, Science Direct, and SpringerLink).

All retrieved studies were screened based on titles and abstracts. Full-text screening was then conducted to ensure alignment with the inclusion criteria. The screening process was performed systematically to maintain consistency and minimize bias.

C. Quality Assessment

The quality of the selected criteria was evaluated using the Joanna Briggs Institute checklist. It emphasizes validity, reliability, systematic clarity, and applicability of the study goals.

1. Reliability: Whether the study employed sound methodology, clear objectives, and reproducible results.
2. Relevance: Whether the study directly addressed IoT applications in healthcare, with findings applicable to the review's research questions.
3. Academic credibility: Whether the study was published in a peer-reviewed journal or conference proceedings, with appropriate citations and theoretical grounding.

Each of the three criteria was scored on a 3-point scale (0 = not met, 1 = partially met, 2 = fully met). Their total score determined the overall quality rating.

Total Score	Rating
5-6	High
3-4	Moderate
0-2	Low

Table I: Rating Table

Example scoring for a typical study (e,g. Verdejo Espinosa et al., 2021):

- Reliability (clear objectives, reproducible) – 2
- Relevance (directly address IoT in RPM) – 2
- Academic credibility (strong citations, peer-reviewed) – 2

Total = 6 (High)

All 15 included studies were rated independently by two reviewers. Disagreements were resolved through discussion. No studies were excluded based on quality alone, but the assessment informed the weight given to findings in the synthesis.

D. Data Extraction

Key information from each of the 15 included studies was extracted and organized using a standardized form. The extracted elements are summarized in Table II.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Table II: Data Extraction Summary

Author	Key Findings	Application	Challenges	Future Direction
Ahmad et al. (2023)	AI aids clinical decisions; positive student views	Telemedicine/AI	Ethics, training, acceptance.	Integrate AI into curricula; user-centered design.
Alaba et al. (2025)	Cross-country differences in infrastructure/regulations	Global IoT healthcare Systems	Privacy laws (HIPAA, GDPR), cost, infrastructure gaps.	Standardized frameworks; context-specific guidelines.
Al-kahtani et al. (2022)	IoT enables dependable remote monitoring during pandemic.	RPM/COVID-19	Security, reliability, interoperability.	Stronger security; clinical workflow integration.
Anmulwar et al. (2020)	Sensor growth, energy use, data quality loss.	Technical challenges	Processing load, energy, transmission errors.	Energy-efficient sensors; robust algorithms.
Babu et al. (2016)	Continuous monitoring reduces manual checks and hospital stays.	RPM	Complexity, cost.	Scalable, low-cost solutions.
Cha et al. (2018)	Privacy enhancing techniques (PETs) protect IoT data	Privacy	Privacy risks, lack of standardized PETs.	Healthcare-specific PETs; regulatory alignment.
Chalapathi et al. (2021)	Edge/fog enable scalable, responsive IoT networks	Edge / fog computing	Deployment challenges, infrastructure needs.	Real-world pilots; AI integration.
Dian et al. (2020)	Wearables attach, implant, or integrate; seamless phone communication.	Wearables	Data overload, user acceptance, integration.	User-centric design; better analytics.
Karalis (2024)	AI applications across specialties; processes large datasets.	AI in clinical practice	Validation, bias, training.	Explainable AI; rigorous trials.
Khan et al. (2022)	Blockchain improves IoT security and trust.	Security/Blockchain	Standardization, scalability.	blockchain; interoperability standards.
Li et al. (2024)	Real-time tracking of patients, staff, equipment.	IoT applications	Interoperability, data management, cost.	Integrated platforms; AI analytics.
Thummarakoti, S., HCA Healthcare (2025)	AI-driven compliance framework for GDPR/HIPAA in cloud systems.	Regulatory compliance	Compliance barriers, cross-border complexity, legacy integration.	Automated compliance; cloud-native architectures.
Espinosa et al. (2021)	Improves asset tracking, efficiency, supports SDGs.	Smart hospitals	Legacy system integration, sustainability.	Sustainable architecture; long-term evaluation.
Zakerabasali & Ayyoubzadeh (2022)	Consent, bias, boundaries	Ethics	Consent, bias, professional-personal blurring.	Ethical frameworks; responsible use guidelines.
Zarkia & Usman (2025)	Weak encryption and insecure firmware cause breaches.	Security/Privacy	Weak encryption, insecure firmware, no standards.	Mandatory security standards; regular updates.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Table III: Thematic Synthesis of Reviewed Studies

Category	Common Issues/Topic	Key Findings	No. of Studies
Applications and Benefits	RPM, Smart hospitals, Telemedicine, Wearables	Improves monitoring and healthcare efficiency	8
Challenges	Interoperability, security, privacy, cost, infrastructure	Major barriers affecting IoT in healthcare systems	15
Future Directions	AI, Edge Computing, Blockchain, PETs	Enables secure and scalable healthcare systems	9

The thematic synthesis reveals that out of 15 reviewed studies, all identify major challenges including interoperability, security, privacy, cost, and infrastructure as barriers to IoT adoption. Eight studies report benefits across RPM, smart hospitals, telemedicine, and wearables, collectively improving monitoring and healthcare efficiency. Nine studies point to future directions involving AI, edge computing, blockchain, and PETs as enablers of secure and scalable systems.

E. Data Analysis and Categorization Framework

The analysis employed a thematic categorization approach. Each of the 15 selected studies was thoroughly reviewed and summarized based on its contribution to three predefined themes:

1. Applications and Benefits of IoT in Healthcare: Wearable devices, remote patient monitoring, and smart hospital systems enable real-time data access, improve patient monitoring, and enhance cost-efficiency.
2. Challenges and Limitations: Interoperability, high implementation costs, technical complexities.
3. Future Security and Privacy Solutions: Blockchain, privacy-enhancing technologies (PETs), standardized security protocols, and regulatory alignment (e.g., HIPAA/GDPR).

IV. RESULTS AND DISCUSSIONS

The synthesis of the 15 selected studies provides a coherent but critical picture of IoT in healthcare: while technological capabilities are well-established, their real-world effectiveness remains constrained by systemic and implementation-level factors. This section moves beyond descriptive reporting by examining how these constraints shape the actual impact of IoT applications.

A. Major IoT Applications and Benefits

The findings consistently identify three dominant application domains—remote patient monitoring (RPM), smart healthcare management, and telemedicine. However, a key analytical insight is that the benefits associated with these applications are conditional rather than inherent.

Remote patient monitoring is widely recognized for enabling continuous tracking of patient health and early detection of abnormalities. While this capability is frequently presented as transformative, its effectiveness depends heavily on the healthcare system's ability to process and respond to continuous data streams. Without sufficient analytical support and workflow integration, continuous monitoring risks generating excessive data without improving clinical outcomes.

Similarly, smart healthcare management systems demonstrate potential in improving operational efficiency through asset tracking and environmental monitoring. However, these improvements are often constrained by integration challenges with legacy hospital systems, resulting in fragmented rather than unified data environments. This suggests that efficiency gains are not solely dependent on IoT deployment but on the extent of institutional readiness for digital integration.

In telemedicine, IoT enhances remote diagnosis and expands access to care, particularly in underserved regions. Nevertheless, its effectiveness is highly dependent on network reliability and infrastructure stability, which vary significantly across healthcare settings. This reinforces the observation that IoT applications are context-dependent, with outcomes shaped by external infrastructural conditions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

B. Recurring Challenges

The analysis reveals that the challenges associated with IoT in healthcare—particularly interoperability, security, privacy, and scalability—are not isolated technical issues but interconnected system-level constraints.

Interoperability remains a central barrier, as the lack of standardized communication protocols across devices creates data silos. This fragmentation limits the ability to generate comprehensive patient records and undermines the potential for integrated, data-driven healthcare. Importantly, interoperability issues also amplify other challenges, including security vulnerabilities and regulatory complexity.

Security and privacy concerns are consistently identified across all studies, reflecting the increased exposure of sensitive patient data within distributed IoT networks. Weak encryption, insecure firmware, and inconsistent security standards contribute to this vulnerability. Moreover, compliance with regulatory frameworks such as HIPAA and GDPR introduces additional complexity, particularly in cloud-based and cross-border data environments.

Scalability further complicates implementation. While many studies report successful pilot systems, there is limited evidence of long-term, large-scale deployment. Issues such as data overload, energy consumption, and network reliability become more pronounced as systems expand, indicating that scalability remains an unresolved challenge rather than an achieved outcome.

C. Research Gaps and Future Directions

The systematic analysis of the 15 reviewed papers confirms and extends the research gaps initially identified in the introduction. While the fragmented nature of the literature was anticipated, this review reveals deeper structural issues within each gap that warrant targeted future investigation.

1. Fragmented Themes Require Integrated Frameworks – Consistent with the observation that few studies combine applications, challenges, and emerging technologies into a single framework, this review found that only 3 of 15 papers attempted such integration [11], [13], [14]. Most studies focused narrowly on either technical development or security, within the attention of clinical integration. Future research must therefore prioritize the development of standardized, modular frameworks that unify application functionality, security-by-design principles, regulatory compliance, and AI-driven analytics into a cohesive healthcare system model [11].

2. Regulatory and ethical alignment remains underspecified – Although privacy concerns were discussed in 10 of the 15 papers, only two provided substantive analysis of ethical obligations or practical compliance with regulations like HIPAA and GDPR [12], [14]. Future work should investigate privacy-enhancing technologies specifically designed to meet healthcare regulatory requirements [6], [12].

3. Scalability and sustainability lack empirical foundation – Emerging technologies (AI, edge computing, PETs) were mentioned in 12 papers, yet only four provided preliminary data on long-term integration [2], [13]. Future research must explore scalable and sustainable IoT architectures that are energy-efficient and maintainable with local expertise [7], [14].

4. Practical implementation barriers are understudied – Interoperability,
were acknowledged as challenges in 13 papers, but detailed analyses in diverse healthcare settings were rare. Notably, studies from low- and middle-income countries were almost entirely absent [2]. Future research should prioritize real-world pilot implementations with long-term evaluation protocols [2], [4], [13].

V. CONCLUSION

This systematic review synthesizes 15 peer-reviewed studies (2015–2025) to examine how IoT functions within healthcare systems beyond its technical capabilities. Rather than treating applications as isolated successes, the analysis demonstrates that the effectiveness of IoT in domains such as remote patient monitoring, smart healthcare management, and telemedicine is structurally contingent on how these technologies are integrated into clinical workflows and data infrastructures.

The findings show that key barriers—interoperability limitations, security and privacy vulnerabilities, infrastructural variability, and regulatory complexity—operate not as discrete challenges but as a coupled constraint system. Interoperability gaps fragment data environments, which in turn complicate security enforcement and regulatory compliance, ultimately limiting scalability. This interdependence explains why many implementations remain confined to pilot settings: expansion amplifies these constraints rather than resolving them.

Consistent with the thematic and cross-study analysis, the review identifies a persistent misalignment in the literature between innovation-focused development and implementation feasibility. Emerging technologies such as artificial intelligence, edge computing, and privacy-enhancing mechanisms are frequently proposed as solutions; however, the evidence indicates that they primarily redistribute system complexity rather than eliminate it. Their effectiveness depends on coordinated integration within existing healthcare architectures, not on standalone deployment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Accordingly, this study contributes an analytical synthesis that links technological functions with system-level behavior, highlighting that IoT outcomes are shaped by interactions across technical, clinical, and regulatory domains. This perspective shifts the focus from individual technologies to the conditions under which they produce meaningful clinical impact.

Future research should therefore prioritize the design and validation of integrated, standards-based architectures, with emphasis on interoperability-by-design, embedded security, and regulatory alignment. Long-term, real-world evaluations across diverse and resource-constrained settings are essential to assess scalability and sustainability. Without addressing these structural conditions, continued innovation is unlikely to translate into consistent, large-scale improvements in healthcare delivery.

VI. BIOGRAPHICAL DATA

Almohairie Agao Bantas is a third-year Bachelor of Science in Computer Engineering student at the University of Southern Mindanao. He completed his secondary education at Southern Baptist College under the STEM strand, graduating with honors, and was recognized for his academic performance at Datu Ibrahim Paglas Memorial College. His interests lie in the development and application of computing technologies, particularly in real-world engineering contexts.

John Lawrence Rodolfo Tobias is a third-year Bachelor of Science in Computer Engineering student at the University of Southern Mindanao. He graduated with honors from Notre Dame of Tacurong College under the Science, Technology, Engineering, and Mathematics (STEM) strand and demonstrated consistent academic excellence at Mamali Elementary School. His interest centers on systems development and applied computing, with an interest in technology-driven solutions.

Vhon Bryan Buhat Silvano is a graduate of Bachelor of Science in Computer Engineering and a Certified Computer Engineer who graduated Cum Laude. He placed 3rd in an in-house research competition at the College of Engineering and Information Technology (CEIT) in 2022. His work demonstrates strengths in systems and applied engineering.

REFERENCES

[1] M. N. Ahmad, S. A. Abdallah, S. A. Abbasi, and A. M. Abdallah, "Student perspectives on the integration of artificial intelligence into healthcare services," *Digital Health*, vol. 9, p. 20552076231174095, 2023.
[2] F. A. Alaba, A. Rocha, H. A. Sulaimon, and O. Najeem, "IoT applications and challenges in global healthcare systems: A comprehensive review," *Future Internet*, vol. 17, no. 12, 2025.
[3] M. S. Al-Kahtani, F. Khan, and W. Taekeun, "Application of Internet of Things and sensors in healthcare," *Sensors*, vol. 22, no. 15, p. 5738, 2022. doi: 10.3390/s22155738.
[4] S. Anmulwar, A. K. Gupta, and M. Derawi, "Challenges of IoT in healthcare," in *IoT and ICT for Healthcare Applications*, Cham: Springer International Publishing, 2020, pp. 11-20.
[5] B. S. Babu, K. Srikanth, T. Ramanjaneyulu, and I. L. Narayana, "IoT for healthcare," *International Journal of Science and Research*, vol. 5, no. 2, pp. 322-326, 2016.
[6] S. C. Cha, T. Y. Hsu, Y. Xiang, and K. H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2159-2187, 2018.
[7] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya, "Industrial internet of things (IIoT) applications of edge and fog computing: A review and future directions," in *Fog/Edge Computing for Security, Privacy, and Applications*, 2021, pp. 293-325.
[8] F. J. Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey," *IEEE Access*, vol. 8, pp. 69200-69211, 2020.
[9] V. D. Karalis, "The integration of artificial intelligence into clinical practice," *Applied Biosciences*, vol. 3, no. 1, pp. 14-44, 2024.
[10] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679-122695, 2022.
[11] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of IoT applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, 2024.
[12] Thummarakoti, S. (2025, March). Compliance and Regulatory Challenges in Cloud-Based Healthcare Systems. In *SoutheastCon 2025* (pp. 1264-1269). IEEE.
[13] Á. Verdejo Espinosa, J. L. Lopez, F. Mata Mata, and M. E. Estevez, "Application of IoT in healthcare: Keys to implementation of the sustainable development goals," *Sensors*, vol. 21, no. 7, p. 2330, 2021.
[14] S. Zakerabasali and S. M. Ayyoubzadeh, "Internet of Things and healthcare system: A systematic review of ethical issues," *Health Science Reports*, vol. 5, no. 6, p. e863, 2022.
[15] M. N. H. Zarkia and S. Usman, "IoT data breaches and privacy issues in healthcare system," *Open International Journal of Informatics*, vol. 13, no. 1, pp. 41-55, 2025.