IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Internet of Things in Smart Healthcare: A Literature Review

Shraddha Hande[1], Pruthviraj Bhosale[2], Samarth Jadhav[3], Sarvesh Kakade[4]
Faculty Mentor, Department of Information Technology[1]
Diploma Students, Department of Information Technology[2,3,4]
Government Polytechnic Awasari (Khurd), Pune, Maharashtra, India
Pruthviraj Bhosale: bpruthviraj248@gmail.com; Samarth Jadhav: samarthjadhav1033@gmail.com;
Sarvesh Kakade: kakadesarvesh2021@gmail.com

Abstract: *Healthcare is slowly shifting from the occasional clinic visit toward care that carries on at home and on the ward between visits. In this paper we review how the Internet of Things (IoT) supports that shift through wearable and implanted sensors, home medical devices, wireless networks, edge gateways and cloud platforms. We drew on thirty-two sources, from journals and clinical trials to standards and Government of India reports. Our reading is that connected monitoring can reduce lost hospital days and improve disease control, but only when a clinical team acts on the data; one large heart-failure trial showed clear benefit and another showed none. The problems reported most often are wireless attacks on implanted devices, sensors that are less accurate during movement or for some patients, alert overload, poor interoperability, battery life, cost and weak rural coverage. In India, eSanjeevani and the Ayushman Bharat Digital Mission now give connected devices somewhere to send their data. We argue that IoT in healthcare should be judged by clinical outcomes, security and fairness rather than by the number of devices connected, and we end with practical suggestions for developers and hospitals.*

Keywords: Internet of Things; smart healthcare; Internet of Medical Things; remote patient monitoring; wearable sensors; edge computing; medical device security; telemedicine

I. INTRODUCTION

A. Background and Motivation

For most people, healthcare still happens in short visits. A doctor checks the blood pressure for a few minutes, and the next reading may come months later, so what happens in between is largely unknown. IoT tries to close that gap: small sensors on the body, in the home or inside the chest take regular readings and send them over a network to software that stores and analyses them. Ashton first used the phrase in 1999 for RFID-tagged objects [1], and Atzori et al. [2] and Gubbi et al. [3] later set out the general architecture of sensing, networking and cloud processing.

Applied to medicine, this is often called the Internet of Medical Things or smart healthcare [4], [5]. Chronic diseases such as heart failure and diabetes change from day to day, and big-data methods promise to turn a steady stream of readings into decisions [6]. In India, eSanjeevani crossed 50 crore teleconsultations in September 2026 [7], and ABDM reports over 104 crore health records linked to more than 93 crore health accounts [8]. The risks are real too: pacemakers have been shown open to wireless attack, sensors are not equally accurate for everyone, alerts can overwhelm small teams, and trials have not always shown benefit.

B. Research Questions

We ask four questions. RQ1: Which technologies make up an IoT healthcare system? RQ2: Which applications are documented, and on what evidence? RQ3: What benefits and limits appear, especially for security, privacy, accuracy,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

cost and interoperability? RQ4: Which gaps remain? Sections V to VIII address RQ1 and RQ2, Sections IX to XI RQ3, and Sections XII to XIV RQ4.

C. Scope and Contribution

Earlier reviews usually cover one layer or one problem: IoT architecture [2], [3], [9], healthcare IoT services [4], [5], big data [6] or sensor-network security [20]. We bring engineering and clinical evidence together for engineering students, keep trial results apart from vendor claims, and give problems as much space as promise. This is a narrative review with no experiments of our own.

II. LITERATURE REVIEW

The sources fall into four groups: IoT foundations, healthcare architectures, clinical evidence, and security, accuracy and governance. Table I summarises the main studies.

A. Foundational Concepts and Surveys

Atzori et al. [2] described IoT as the meeting of things, internet and data, and named security and privacy as open problems. Gubbi et al. [3] proposed a cloud-centric vision with healthcare as a leading use, and Al-Fuqaha et al. [9] surveyed protocols such as MQTT and CoAP. Kvedar et al. [10] argued that connected health works only when it fits how patients and clinicians actually work.

B. Healthcare IoT Surveys and Architectures

Islam et al. [4] surveyed healthcare IoT services and gave a taxonomy of attacks. Baker et al. [5] proposed a generic model of sensors, links and cloud, naming power and standards as obstacles. Dimitrov [6] stressed turning data into decisions, and Rahmani et al. [11] showed that an edge gateway can filter data and keep alerts working when the internet link drops.

C. Clinical Evidence for Remote Monitoring

In the TIM-HF2 trial, Koehler et al. [12] randomised 1,538 heart-failure patients in Germany. Those who sent daily weight, blood pressure, ECG and oxygen readings to a round-the-clock telemedical centre lost 4.88% of days to unplanned admission or death against 6.64% with usual care, and had lower all-cause mortality (hazard ratio 0.70). BEAT-HF [13], with 1,437 patients in California, found no change in 180-day readmission. An implanted pulmonary artery sensor cut heart-failure hospitalisations by about 28% at six months in 550 patients [14], and continuous glucose monitoring lowered HbA1c by 1.0% against 0.4% in 158 adults with type 1 diabetes [15]. Monitoring seems to help when someone has a clear way to act on the data.

D. Wearables and Consumer Devices

The Apple Heart Study [16] followed 419,297 smartwatch users; 0.52% were notified of an irregular pulse, and notifications matched atrial fibrillation on ECG with a positive predictive value of 0.84. Bent et al. [17] found no skin-tone effect in wearable heart-rate accuracy but about 30% more error during activity. Sjoding et al. [18] found hidden low oxygen in 11.7% of Black patients against 3.6% of White patients whose oximeters read 92% to 96%.

E. Security and Privacy

Halperin et al. [19] reprogrammed an implanted defibrillator over its radio in 2008. Kumar and Lee [20] listed the security needs of low-power medical sensor networks, and the Mirai botnet [21] showed how default passwords expose IoT devices. In 2017 Abbott issued a firmware update for about 465,000 US pacemakers after security flaws were confirmed [22].

F. Artificial Intelligence and Emerging Directions

Hannun et al. [23] trained a deep network on 91,232 single-lead ECGs from 53,549 patients and reached an F1 score of 0.837 against 0.780 for cardiologists, though on a small retrospective test set. Azaria et al. [24] proposed MedRec, a blockchain prototype for patient-controlled record access.

G. Synthesis of Agreements, Tensions and Gaps

The studies agree that value comes from the whole loop rather than the sensor [12]–[15], that security must be designed in from the start [4], [19], [20], and that processing near the patient is increasingly needed [11], [25], [26]. The tensions

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

are that wearables create follow-up work and vary in accuracy [16]–[18], and that most trials come from well-staffed health systems, not district hospitals with patchy coverage.

TABLE I: SUMMARY OF PRINCIPAL REVIEWED STUDIES ON IOT IN SMART HEALTHCARE

Study and Ref.	Primary Objective	Approach	Scope or Sample	Key Reported Findings	Principal Limitations
Baker et al. [5]	Propose a smart healthcare model	Survey and model	Sensors, links and cloud	Power, standards and security are main challenges	No clinical test
Rahmani et al. [11]	Use fog gateways in healthcare IoT	Prototype	Smart e-health gateway	Less delay and cloud traffic; works offline	No patient outcomes
Koehler et al. [12]	Test remote management in heart failure	RCT	1,538 patients, Germany	Days lost 4.88% vs 6.64%; fewer deaths	Needs 24-hour centre
Ong et al. [13]	Test telemonitoring after discharge	RCT	1,437 patients, California	No change in 180-day readmission	Incomplete adherence
Beck et al. [15]	Test continuous glucose monitoring	RCT	158 adults, type 1 diabetes	HbA1c fell 1.0% vs 0.4%	24-week follow-up
Perez et al. [16]	Screen for AF with a smartwatch	Virtual cohort	419,297 users	0.52% notified; PPV 0.84	Many lost to follow-up
Sjoding et al. [18]	Check bias in pulse oximetry	Retrospective cohort	Two US cohorts	Hidden low oxygen 11.7% vs 3.6%	Hospital data
Halperin et al. [19]	Test wireless security of an ICD	Laboratory attack	One ICD model	Device read and reprogrammed by radio	Short range

Source: Compiled by the authors from the cited publications. Findings are reported as stated by the original authors.

III. OBJECTIVES OF THE STUDY

- Explain the layers of an IoT healthcare system and how they work together (Section V).
- Document uses in patient care (Section VI) and hospitals (Section VII), and compare documented examples (Section VIII).
- Weigh benefits against limits in security, privacy, accuracy, cost and interoperability (Sections IX to XI).
- Identify gaps and give practical recommendations (Sections XII to XIV).

IV. RESEARCH METHODOLOGY

A. Review Design and Information Sources

We followed a narrative review design, reading surveys, trials, laboratory studies and government reports side by side without pooling results. We began with three widely cited surveys [2], [4], [5] and extended the list through IEEE Xplore, PubMed, publisher sites and Government of India portals in October 2026.

B. Search Strategy, Screening Criteria and Appraisal

Search terms included IoT healthcare, remote patient monitoring, continuous glucose monitoring, wearable accuracy, pacemaker security, fog computing, eSanjeevani and ABDM. We preferred peer-reviewed trials and kept a source only if its method and sample were clear. Government and press reports [7], [8], [22] are used only for context, and key figures from [7], [12], [16] and [18] were checked against the originals.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

V. TECHNOLOGY FOUNDATIONS

A. Historical Development

The term IoT came from RFID in 1999 [1], security warnings arrived early with a 2008 attack on an implanted defibrillator [19], large trials followed in the 2010s, and recent years have brought wearables, AI and national digital health platforms in India [7], [8] (Table II).

TABLE II: SELECTED MILESTONES IN THE DEVELOPMENT OF IOT FOR HEALTHCARE

Year	Milestone	Why It Matters for Smart Healthcare
1999–2013	IoT term coined [1]; ICD wireless attack [19]; IoT surveys [2], [3]	Shared vocabulary; security becomes a safety issue
2011–2017	Implanted sensor trial [14]; IEEE 802.15.6 [27]; fog computing [25]; DIAMOND [15]; Mirai [21]; pacemaker recall [22]	Clinical evidence and public security concern
2018–2020	TIM-HF2 [12]; Apple Heart Study [16]; AI ECG [23]; oximetry bias [18]	Large trials; accuracy and fairness in focus
2021–2026	ABDM (2021); DPDP Act [31]; eSanjeevani passes 50 crore [7]	National infrastructure and data law in India

Source: Compiled by the authors from the cited studies and public records.

B. Perception Layer: Sensors and Devices

Wearables measure heart rate, oxygen, ECG and movement; home devices include blood-pressure cuffs, scales and glucose monitors; implants include pacemakers and pressure sensors [14]; RFID tags track equipment. Accuracy depends on placement, movement and the wearer [17], [18].

C. Network Layer

BLE, Zigbee and IEEE 802.15.6 [27] link sensors to a phone or gateway at low power; Wi-Fi serves homes and wards; 4G/5G, NB-IoT and LoRaWAN cover rural distances; MQTT and CoAP carry small messages [9] (Table III).

D. Edge, Fog and Cloud Processing

Fog [25] and edge computing [26] move processing close to the patient, so a gateway can raise an alarm within seconds even offline [11], while the cloud handles storage and analytics (Fig. 1).

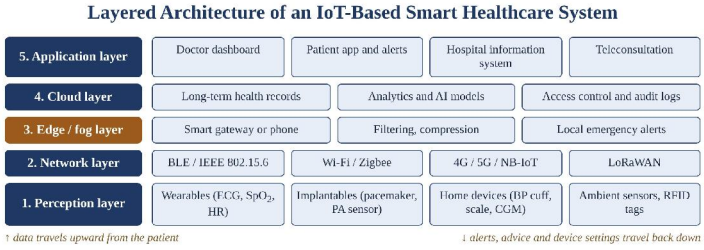


Fig. 1. Layered architecture of an IoT-based smart healthcare system. Adapted from [3], [5] and [11]; the examples in each layer are illustrative.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

TABLE III: COMPARISON OF COMMUNICATION TECHNOLOGIES USED IN HEALTHCARE IOT

Dimension	Short-Range Body Network	Local Network (Wi-Fi, Zigbee)	Wide-Area Network (4G/5G, NB-IoT, LoRaWAN)
Range	A few metres around the body	A house or hospital floor	A town or district
Power use	Very low; suits coin cells	High for Wi-Fi; low for Zigbee	Very low for NB-IoT and LoRaWAN
Main limits	Needs a phone or gateway nearby	Interference; coverage gaps	Data cost; patchy rural coverage

Source: Authors' synthesis of [5], [9] and [27].

E. System Components and Working Process

Table IV lists the main components, and Fig. 2 the loop from sensing to clinical response. Urgent alerts belong at the edge [11], while daily trends can be reviewed later [12]. HL7 FHIR [30] gives devices and hospital systems a common data model.

TABLE IV: MAIN COMPONENTS OF AN IOT-BASED SMART HEALTHCARE SYSTEM

Component	Purpose	Typical quality concern
Sensor or implant	Measures a vital sign or treats from inside the body	Accuracy; battery; wireless security
Gateway or smartphone	Collects data, runs edge rules, forwards it	Pairing failures; app updates
Cloud platform	Stores records and runs analytics	Privacy, availability, lock-in
Clinical dashboard	Flags patients to staff	Alert overload; who responds

Source: Authors' synthesis of the cited literature.

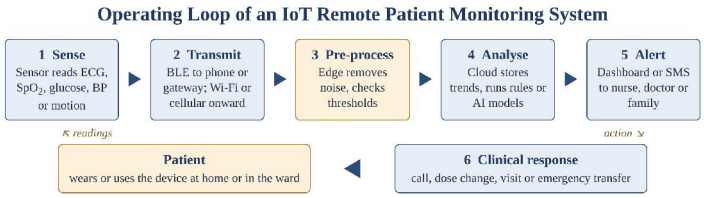


Fig. 2. Operating loop of an IoT remote patient monitoring system. Data that is collected but not acted on adds cost without benefit.

VI. APPLICATIONS IN PATIENT CARE

A. Remote Monitoring in Heart Failure

TIM-HF2 [12] paired home readings with doctors who could act at any hour and reduced days lost; BEAT-HF [13] relied on nurse review and coaching and did not; the implanted sensor [14] avoided daily effort at the cost of a procedure. The technology was similar; the organisation of the response was not.

B. Diabetes and Continuous Glucose Monitoring

A thin sensor under the skin reports glucose every few minutes to a phone, with low-glucose alarms and sharing with family, and improved HbA1c over 24 weeks [15].

C. Cardiac Rhythm Screening with Wearables

Smartwatches can flag possible atrial fibrillation at scale [16], and AI could read wearable ECGs [23], but each alert needs follow-up that many users never complete.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, October 2026 Impact Factor: 8.2

D. Elderly Care and Fall Detection

Wearable, ambient and camera-based fall detectors often perform worse in real homes than in tests, and false alarms and privacy reduce acceptance [28].

E. Post-Discharge and Pandemic Home Monitoring

Home pulse oximeters were widely used during COVID-19, but if they over-read for some patients [18], fixed thresholds can miss the people most at risk.

F. Artificial Intelligence on Health IoT Data

Models running on the gateway can cut delay [11], [26] and combine signals with records [6], but they need prospective validation across ages, devices and populations [23].

VII. APPLICATIONS IN HOSPITALS AND HEALTH SYSTEMS

A. Asset and Patient Tracking with RFID

RFID helps track equipment, patients, specimens and drugs, though cost, interference and privacy remain barriers [29].

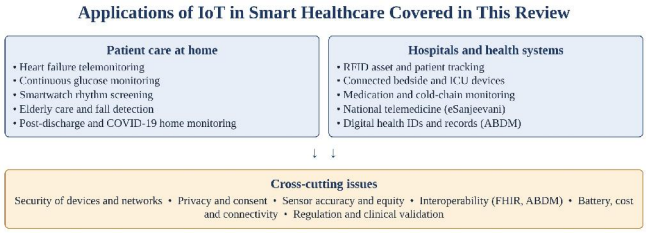


Fig. 3. Applications of IoT in smart healthcare covered in this review, with the issues that cut across all of them.

B. Connected Bedside and ICU Devices

Networked monitors and pumps save nursing time but often run old, unpatched software [4], [21] and add to alarm fatigue.

C. Medication Management and Cold Chain

Smart pill boxes record adherence, and connected temperature loggers protect vaccines and insulin in transit.

D. National Telemedicine in India

eSanjeevani links primary-care spokes with doctors at hubs and now offers specialist consultations and AI decision support [7]; shared connected devices at spokes may suit rural India better than personal wearables.

E. Digital Health IDs and Records

ABDM links records to a 14-digit health account with consent [8], so device readings could join a lifelong record, subject to data law [31] and common standards [30].

VIII. DOCUMENTED EXAMPLES AND PLATFORMS

Table V separates peer-reviewed evidence from government and press figures that we could not verify ourselves.

TABLE V: DOCUMENTED EXAMPLES OF IOT IN SMART HEALTHCARE AND THE EVIDENCE AVAILABLE FOR EACH

Example (Developer, Year)	Technology	Healthcare Use	What Is Documented	Evidence Type	Reported Constraint
TIM-HF2 (Charité Berlin, 2018)	Home vital-sign devices	Heart-failure monitoring	Days lost 4.88% vs 6.64% [12]	Peer-reviewed RCT	24-hour centre needed

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

CardioMEMS (2011)	Implanted pressure sensor	Heart-failure management	About 28% fewer hospitalisations [14]	Peer-reviewed RCT	Invasive; costly
Apple Watch (Apple and Stanford, 2019)	Optical smartwatch sensor	AF screening	0.52% notified; PPV 0.84 [16]	Peer-reviewed cohort	Incomplete follow-up
Abbott RF pacemakers (2017)	Implanted pacemaker	Pacing with remote follow-up	Update for about 465,000 devices [22]	Press report	Clinic visit needed
eSanjeevani (MoHFW, C-DAC)	Telemedicine platform	Teleconsultation	50 crore consultations [7]	Government report	Usage, not outcomes

Source: Compiled by the authors from the cited studies and public reports.

IX. COMPARATIVE DISCUSSION

A. Traditional and IoT-Enabled Care

TABLE VI: COMPARISON OF TRADITIONAL AND IOT-ENABLED HEALTHCARE

Feature	Traditional Care	IoT-Enabled Care	Qualification
Measurement	Occasional clinic readings	Daily or continuous readings	Accuracy varies [17]
Detecting change	At the next visit	Trends flag change early	Only if someone acts [13]
Security risk	Physical access to records	Remote attack on devices [19]	Long-term patching needed
Access	Limited by distance	Reaches rural homes [7]	Needs coverage and skills

Source: Authors' synthesis of the reviewed studies.

B. More Data Versus Better Care

More readings allow earlier action [12], [14], [15], but someone must review them and respond, as BEAT-HF shows [13]. Our rule for engineers is to design the response first and the sensor second.

C. Choosing Connectivity and Architecture

BLE and a phone suit urban patients, Wi-Fi suits wards, and NB-IoT gateways with store-and-forward suit rural centres, with urgent alerts decided at the edge [11], [25], [26] and data exported in standard formats [30].

D. Cost, Access and the Indian Context

Most trial evidence comes from Germany and the United States [12]–[16]. The scale of eSanjeevani [7] and ABDM [8] suggests that shared devices at primary-care centres may be a more realistic path for India.

E. Quality of the Evidence

Engineering papers are mostly descriptive, accuracy studies are small [17], and usage figures come from government releases [7], [8].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

F. Measuring IoT Healthcare Systems

TABLE VII: COMMON MEASURES USED TO EVALUATE IOT IN SMART HEALTHCARE

Aspect	Typical Measure	Example from the Reviewed Studies	Caution
Clinical outcome	Hospital days, death	Days lost [12]	Needs large trials
Diagnostic performance	PPV, F1 score	PPV 0.84 [16]; F1 0.837 [23]	Depends on who is tested
Fairness	Error by subgroup	Oximetry by race [18]	Needs diverse cohorts
Security	Ability to alter a device	ICD reprogramming [19]	Lab may differ from field

Source: Authors' synthesis of the reviewed studies.

X. BENEFITS AND CHALLENGES

A. Benefits

- Earlier detection [12], [14]; better diabetes control [15]; screening at scale [16]; rural access [7]; hospital efficiency [29]; linked records [8].

B. Challenges

- Security [19], [22]; privacy [31]; accuracy and fairness [17], [18]; workload [13]; interoperability [5], [30]; power and coverage [11]; cost.

TABLE VIII: SUMMARY OF CONDITIONAL ADVANTAGES AND CORRESPONDING LIMITATIONS OF IOT IN SMART HEALTHCARE

Dimension	Conditional Advantage	Corresponding Limitation or Requirement
Early detection	Daily readings reveal deterioration [12], [14]	Needs a team that responds [13]
Automation	AI screens large data volumes [23]	Not yet validated prospectively
Connectivity	Remote follow-up and updates	Wireless attack surface [19], [22]

Source: Authors' synthesis of the reviewed studies.

XI. SECURITY, PRIVACY, EQUITY AND RESPONSIBLE DESIGN

A. Device and Network Security

Devices may stay in service for a decade, so encrypted links, authentication, signed firmware and no default passwords are basic requirements [4], [19]–[22].

B. Privacy and Consent

The DPDP Act, 2023 [31] requires a lawful basis and purpose limits; ABDM builds consent into sharing [8], and patient-controlled access [24] is promising but immature.

C. Accuracy and Equity

Devices should be validated on Indian users and in real activity before clinical use [17], [18], and programmes should not assume every patient has a smartphone.

D. Interoperability

Closed vendor formats block data sharing [5]; HL7 FHIR [30] should be a purchasing requirement.

E. Regulation and Clinical Validation

CDSCO regulates devices by risk under the Medical Devices Rules, 2017 [32], but connected devices raise new questions about software changes and security updates [22].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

XII. LIMITATIONS, OPEN CHALLENGES AND FUTURE DIRECTIONS

A. Limitations of This Review

This narrative review may miss studies, uses some figures from abstracts and government releases, and runs no experiments.

B. Principal Challenges

- Established: device security [19], [22]; power and rural coverage [5], [11].
- Active or emerging: mixed clinical evidence [12], [13]; sensor fairness [17], [18]; interoperability [30]; clinical AI [23].

C. Future Directions

Fig. 4 maps the gaps to directions: pragmatic trials in Indian primary care linked to national platforms [7], [8], security by design [19], [22], validation on diverse users [17], [18], edge filtering of alerts [11], [26], and prospective testing of AI [23].

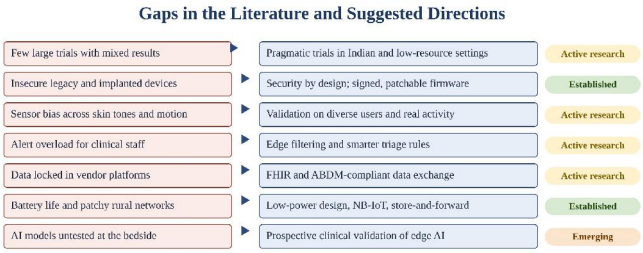


Fig. 4. Gaps identified in the reviewed literature, with suggested research directions and an indication of how mature each topic is.

XIII. CONCLUSION

IoT gives healthcare continuous readings, earlier detection, better disease control and wider access [7], [12], [14]–[16], but these benefits depend on a team that responds, devices that are accurate for their users and reliable connectivity [13], [17], [18]. Security, privacy, interoperability and evidence from low-resource settings remain open [19], [22], [30], [31]. With national platforms in place [7], [8], India's next step is to link devices safely to the care that already exists, and a low-cost prototype tested at a local health centre would be a useful start.

XIV. PRACTICAL RECOMMENDATIONS

A. Guidelines for Developers and Engineers

- Design the response before the sensor [12], [13]; put urgent rules on the edge [11]; secure every device [19], [21].
- Validate accuracy across users [17], [18]; export FHIR data [30]; collect only needed data [31]; use low-power links [5], [27].

B. Guidelines for Hospitals, Researchers and Educators

- Start where evidence is strongest [12], [15]; staff alert review [13]; demand security commitments [22], [32]; run Indian trials [7], [8]; teach the full loop with low-cost kits.

ACKNOWLEDGMENT AND DECLARATIONS

Pruthviraj Bhosale, Samarth Jadhav and Sarvesh Kakade thank Shraddha Hande and the Department of Information Technology at Government Polytechnic, Awasari Khurd, for their academic supervision and guidance. Author contributions: Pruthviraj Bhosale, Samarth Jadhav and Sarvesh Kakade selected the topic, collected and reviewed the literature, organised the discussion and prepared the manuscript; Shraddha Hande supervised the work and reviewed the final manuscript. Conflict of interest and funding: The authors declare no conflict of interest and received no external

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

financial support for this study. Ethical approval: Not applicable, as this study reviews published literature and public reports and involves no human participants or private data.

REFERENCES

[1] K. Ashton, "That 'Internet of Things' thing," RFID J., Jun. 22, 2009.
[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
[4] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.
[5] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
[6] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," Healthc. Inform. Res., vol. 22, no. 3, pp. 156–163, Jul. 2016, doi: 10.4258/hir.2016.22.3.156.
[7] "eSanjeevani crosses 50 crore teleconsultations, marking milestone in India's digital healthcare initiative," All India Radio News, Oct. 6, 2026. [Online]. Available: https://newsonair.gov.in/esanjeevani-achieves-milestone-of-50-cr-teleconsultations-from-across-the-country/ (accessed Oct. 29, 2026).
[8] Press Information Bureau, Government of India, "Ayushman Bharat Digital Mission: India's digital health backbone," Jul. 6, 2026. [Online]. Available: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jul/doc202676912801.pdf (accessed Oct. 29, 2026).
[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
[10] J. Kvedar, M. J. Coye, and W. Everett, "Connected health: A review of technologies and strategies to improve patient care with telemedicine and telehealth," Health Aff., vol. 33, no. 2, pp. 194–199, Feb. 2014, doi: 10.1377/hlthaff.2013.0992.
[11] A. M. Rahmani et al., "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," Future Gener. Comput. Syst., vol. 78, pp. 641–658, Jan. 2018, doi: 10.1016/j.future.2017.02.014.
[12] F. Koehler et al., "Efficacy of telemedical interventional management in patients with heart failure (TIM-HF2): A randomised, controlled, parallel-group, unmasked trial," Lancet, vol. 392, no. 10152, pp. 1047–1057, Sep. 2018, doi: 10.1016/S0140-6736(18)31880-4.
[13] M. K. Ong et al., "Effectiveness of remote patient monitoring after discharge of hospitalized patients with heart failure: The Better Effectiveness After Transition–Heart Failure (BEAT-HF) randomized clinical trial," JAMA Intern. Med., vol. 176, no. 3, pp. 310–318, Mar. 2016, doi: 10.1001/jamainternmed.2015.7712.
[14] W. T. Abraham et al., "Wireless pulmonary artery haemodynamic monitoring in chronic heart failure: A randomised controlled trial," Lancet, vol. 377, no. 9766, pp. 658–666, Feb. 2011, doi: 10.1016/S0140-6736(11)60101-3.
[15] R. W. Beck et al., "Effect of continuous glucose monitoring on glycemic control in adults with type 1 diabetes using insulin injections: The DIAMOND randomized clinical trial," JAMA, vol. 317, no. 4, pp. 371–378, Jan. 2017, doi: 10.1001/jama.2016.19975.
[16] M. V. Perez et al., "Large-scale assessment of a smartwatch to identify atrial fibrillation," N. Engl. J. Med., vol. 381, no. 20, pp. 1909–1917, Nov. 2019, doi: 10.1056/NEJMoa1901183.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, October 2026 Impact Factor: 8.2

[17] B. Bent, B. A. Goldstein, W. A. Kibbe, and J. P. Dunn, "Investigating sources of inaccuracy in wearable optical heart rate sensors," npj Digit. Med., vol. 3, Art. no. 18, Feb. 2020, doi: 10.1038/s41746-020-0226-6.
[18] M. W. Sjoding, R. P. Dickson, T. J. Iwashyna, S. E. Gay, and T. S. Valley, "Racial bias in pulse oximetry measurement," N. Engl. J. Med., vol. 383, no. 25, pp. 2477–2478, Dec. 2020, doi: 10.1056/NEJMc2029240.
[19] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, 2008, pp. 129–142, doi: 10.1109/SP.2008.31.
[20] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2012, doi: 10.3390/s120100055.
[21] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.
[22] M. Mezher, "Abbott recalls 465,000 pacemakers for cybersecurity patch," Regulatory Focus, Regulatory Affairs Professionals Society, Aug. 30, 2017. [Online]. Available: https://www.raps.org/resource/abbott-recalls-465000-pacemakers-for-cybersecurit.html (accessed Oct. 29, 2026).
[23] A. Y. Hannun et al., "Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network," Nat. Med., vol. 25, no. 1, pp. 65–69, Jan. 2019, doi: 10.1038/s41591-018-0268-3.
[24] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
[25] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st MCC Workshop Mobile Cloud Comput., Helsinki, Finland, 2012, pp. 13–16, doi: 10.1145/2342509.2342513.
[26] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.
[27] IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks, IEEE Std 802.15.6-2012, Feb. 2012, doi: 10.1109/IEEESTD.2012.6161600.
[28] R. Igual, C. Medrano, and I. Plaza, "Challenges, issues and trends in fall detection systems," Biomed. Eng. Online, vol. 12, Art. no. 66, Jul. 2013, doi: 10.1186/1475-925X-12-66.
[29] W. Yao, C.-H. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: A literature review," J. Med. Syst., vol. 36, no. 6, pp. 3507–3525, Dec. 2012, doi: 10.1007/s10916-011-9789-8.
[30] HL7 International, "FHIR (Fast Healthcare Interoperability Resources) Release 4." [Online]. Available: https://hl7.org/fhir/R4/ (accessed Oct. 29, 2026).
[31] Ministry of Law and Justice, Government of India, "The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)," The Gazette of India, Aug. 11, 2023.
[32] Ministry of Health and Family Welfare, Government of India, "Medical Devices Rules, 2017," G.S.R. 78(E), Jan. 31, 2017. Administered by the Central Drugs Standard Control Organisation.