Journal of Advanced Research in Data Structures Innovations and Computer Science
Volume 1, Issue 2 - 2025, Pg. No. 8-10
Peer Reviewed Journal

Review Article

IoT in Healthcare Sector and Smart Home Appliances Applications

Kishan Sagpariya[1], Shlok Vekariya[2]

[1]Student, Department of Mechanical Engineering, V V P Engineering College, Kalawad Road, Rajkot, Gujarat, India
[2]Student, Department of Electronics and Communication Engineering, CSPIT, Nadiad-Petlad Road, Changa, Gujarat
DOI: https://doi.org/10.24321/3051.438X.202501

I N F O

Corresponding Author:
Kishan Sagpariya, Department of Mechanical Engineering, V V P Engineering College, Kalawad Road, Rajkot, Gujarat, India
E-mail Id:
kishan.sagpariya701@gmail.com
Orcid Id:
https://orcid.org/0009-0008-0363-3600
How to cite this article:
Sagpariya K, Vekariya S. IoT in Healthcare Sector and Smart Home Appliances Applications. *J Adv Res Data Struct Innov Comput Sci* 2025; 1(2): 8-10.

Date of Submission: 2025-08-14
Date of Acceptance: 2025-09-05

A B S T R A C T

The Internet of Things (IoT) is rapidly transforming the digital ecosystem by enabling smart, connected environments across various domains. Among its most impactful applications are IoT in healthcare and smart homes, where real-time data exchange and automation are improving quality of life and service delivery. However, as IoT systems scale, they also face critical challenges—notably in terms of security, data integrity, interoperability, and privacy. In the healthcare domain, IoT facilitates innovations such as remote patient monitoring, wearable health devices, and AI-driven diagnostics, allowing for continuous care and early detection of anomalies. In smart homes, IoT enables automation, energy efficiency, voice-activated controls, and enhanced safety. While these advancements offer immense potential, they also require robust frameworks to ensure data protection and system reliability.

Keywords: Healthcare, IoT Smart Homes, Security Challenge, Data Privacy Challenge, Automation

Introduction

The Internet of Things (IoT) is a technological revolution that connects physical devices to the internet, enabling them to collect, transmit, and analyse data in real time. With over 14 billion connected devices globally and projections reaching 30 billion by 2030, IoT is rapidly reshaping sectors ranging from agriculture to urban infrastructure.[1] Two of the most impactful areas of IoT implementation are the healthcare sector and smart home systems.

In healthcare, IoT enables continuous patient monitoring, early diagnosis, and efficient management of resources. Smart homes, on the other hand, leverage IoT to enhance comfort, security, energy efficiency, and convenience through automation and intelligent control. Despite these advantages, widespread IoT adoption presents major challenges, especially around data privacy, interoperability, and cybersecurity.[2]

Iot In The Healthcare Sector

IoT devices in healthcare include wearable fitness trackers, smart inhalers, remote ECG monitors, insulin pens, and telemedicine platforms (figure 1). These systems support Remote Patient Monitoring (RPM), Real-Time Health Analytics, and AI-assisted diagnostics.[3] The block diagram of smart home automation is shown in Figure 2.

Examples:

- Wearables (e.g., Fitbit, Apple Watch) monitor heart rate, oxygen levels, and sleep patterns.
- Smart beds adjust automatically to improve patient comfort and reduce pressure injuries.
- Connected inhalers alert asthma patients to usage patterns and environmental triggers.

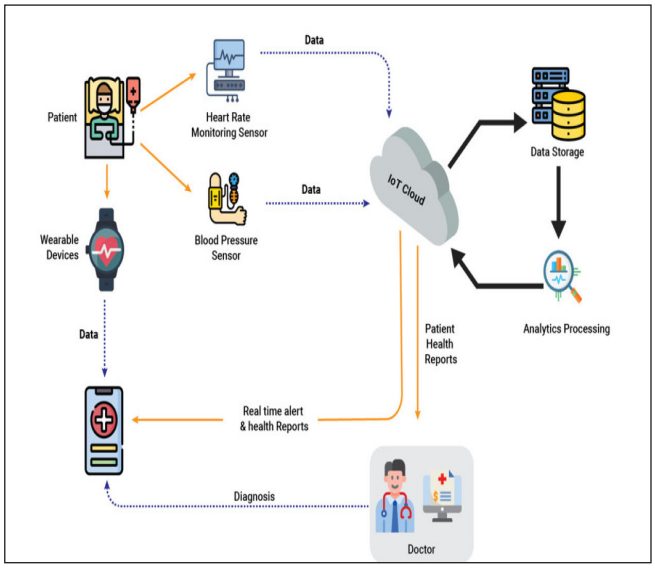

Figure 1.Block diagram of Healthcare IoT System

Benefits

- **Early Diagnosis:** AI algorithms analyse data for early detection of disease.
- **Operational Efficiency:** Hospitals track equipment and optimise staff allocation.
- **Personalised Care:** Data-driven treatment plans improve recovery and satisfaction.

Challenges

- **Data Security:** Medical data is highly sensitive, and breaches can lead to identity theft.
- **Interoperability:** Devices from different manufacturers often lack communication standards.
- **Regulatory Compliance:** Systems must adhere to HIPAA, GDPR, and local laws.[4]

Iot In Smart Home Appliances

Key Applications

- IoT-enabled smart homes provide convenience through automation of household systems such as:
- Lighting (e.g., Philips Hue)
- Thermostats (e.g., Nest)
- Voice Assistants (e.g., Amazon Alexa, Google Assistant)
- Security Systems (e.g., Ring doorbells, smart locks)

Advantages

- **Energy Efficiency:** Smart meter
- Thermostats reduce waste and save electricity.
- **Comfort and Accessibility:** Elderly and disabled individuals benefit from voice-and motion-activated controls.
- **Safety:** Sensors detect gas leaks, smoke, water leaks, and intrusions.

Challenges

- **Privacy Risks:** Voice assistants and cameras may unintentionally collect private data.
- **Cybersecurity:** Devices often have weak passwords or lack software updates.[5]
- **Vendor Lock-in:** Lack of standardisation ties users to a single ecosystem.

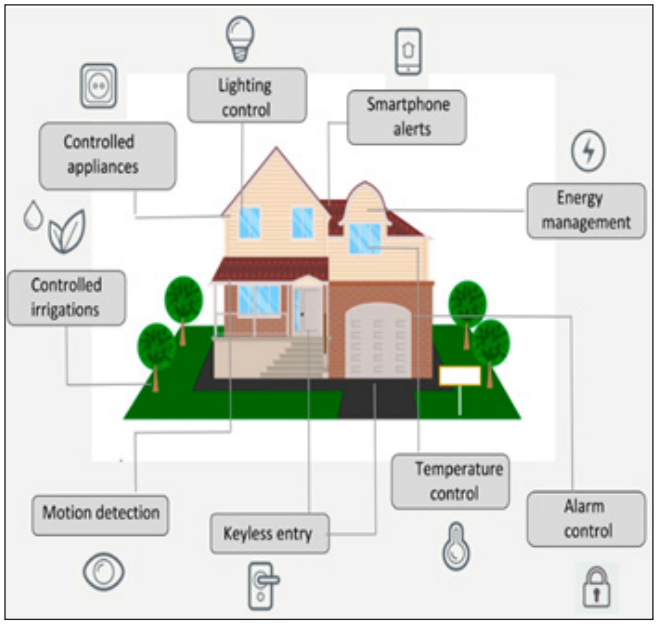

Figure 2.Block diagram of Smart Home Automation)

Data Privacy And Security Challenges

As IoT devices collect vast amounts of data, ensuring its confidentiality, integrity, and availability becomes critical. Common threats include:

- Eavesdropping on unencrypted transmissions.
- Device hijacking to gain access to home or hospital networks.
- Ransomware attacks on hospital IoT systems, putting lives at risk.

Solutions:

End-to-End Encryption

- Secure Boot and Firmware Updates
- Blockchain for Data Integrity[6]

However, implementing these solutions at scale—especially in low-power or legacy devices—remains a challenge.

Emerging Tools

- **Edge Computing:** Processing data closer to the source reduces latency and enhances privacy.

ISSN: 3051-438X
DOI: https://doi.org/10.24321/3051.438X.202501

- **AI and Machine Learning:** Enable predictive analytics for proactive care and automation.
- **Federated Learning:** Allows models to train on decentralised data without compromising privacy.
- **Matter Protocol:** A universal connectivity standard for smart homes, developed by CSA.[7]
- These trends aim to make IoT ecosystems more secure, interoperable, and user-centric.

Comparative Analysis

- Goal Health monitoring & diagnostics Comfort, efficiency, security
- Key Devices Wearables, monitors, sensors Lights, locks, appliances
- Risk Level High (sensitive data) Moderate
- Privacy Concern Very high Medium to high
- Regulation Required (HIPAA, GDPR) Mandatory Emerging

Conclusion

The integration of Internet of Things (IoT) technologies in the healthcare sector and smart home environments has proven to be a transformative force, revolutionising how services are delivered and experienced. From remote patient monitoring and wearable health devices to automated lighting and voice-controlled appliances, IoT is at the forefront of innovation aimed at improving both health outcomes and quality of life.

However, this rapid adoption comes with significant challenges—data privacy, security, interoperability, and infrastructure reliability must be addressed with equal intensity. Without robust frameworks, the full potential of IoT will remain underutilised or, worse, pose risks to users.

Emerging trends such as AI-enabled diagnostics, edge computing, blockchain for secure data exchange, and federated learning indicate a shift toward more decentralised, intelligent, and privacy-aware IoT ecosystems. These innovations will not only tackle present challenges but also open doors to more personalised, efficient, and ethical implementations in both sectors.

In conclusion, while IoT has already made remarkable strides in healthcare and smart homes, its real power lies ahead—in its ability to learn, adapt, and connect ethically and intelligently. The future belongs to smart systems that put humans at the centre, ensuring security, trust, and accessibility for all.

References

1. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60.
2. Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of things architecture, possible applications and key challenges. In2012 10th international conference on frontiers of information technology 2012 Dec 17 (pp. 257-260). IEEE.
3. Zahabia N. How wearable devices are changing healthcare, 21% of people in the US regularly wear a smartwatch [Internet]. StraitsResearch; 2022 Feb 11 [cited 2025 Aug 17]. Available from: https://straitsresearch.com/article/wearable-devices-future-of-the-healthcare/
4. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing. 2017 Mar 1;21(2):34-42.
5. Zhao K, Ge L. A survey on the internet of things security. In2013 Ninth international conference on computational intelligence and security 2013 Dec 14 (pp. 663-667). IEEE.
6. Conoscenti M, Vetro A, De Martin JC. Blockchain for the Internet of Things: A systematic literature review. In2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) 2016 Nov 29 (pp. 1-6). IEEE.
7. Alliance CS. Matter-the foundation for connected things. URL https://csa-iot. org/all-solutions/matter. 2024 Oct 3.

ISSN: 3051-438X
DOI: https://doi.org/10.24321/3051.438X.202501