Ramakrishnan et al. Scr Med. 2025 May-Jun;56(3):621-4. DOI:10.5937/scriptamed56-55961

LETTER TO THE EDITOR

IoT-Enabled Smart Implants Surgery: Revolutionising Precision, Monitoring and Patient Safety

Praveen Ramakrishnan,[1] Abdulkadhar Mohamed Jalaludeen,[1] Lalitha Gnanasekaran,[2] Thanigaivel Sundaram,[3] Shivani Chopra,[4] Hitesh Chopra[5]

1. Crescent Global Outreach Mission Research and Development, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.
2. Alta Institute of Technology, University of Tarapaca, Arica, Chile.
3. Department of Biotechnology, Faculty of Science & Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu District, Tamil Nadu, India.
4. Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India.
5. Centre for Research Impact and Outcome, Chitkara College of Pharmacy, Chitkara University, Rajpura, Punjab, India.

Citation:
Ramakrishnan P, Jalaludeen AM, Gnanasekaran L, Sundaram T, Chopra S, Chopra H. IoT-enabled smart implants surgery: revolutionising precision, monitoring and patient safety. Scr Med. 2025 May-Jun;56(3):621-4.

Corresponding authors:
SUNDARAM THANIGAIVEL
E: thanigaivel092@gmail.com

HITESH CHOPRA
E: chopraontheride@gmail.com

ARTICLE INFO
Received: 12 January 2025
Accepted: 31 January 2025

Dear Editor,

The integration of Internet of Things (IoT) technology into implant surgery has altered healthcare by transforming implants from passive devices to intelligent, networked systems that enhance surgical outcomes, allow for real-time monitoring and increase post-operative care.[1] IoT-enabled implants have sophisticated sensors that monitor key indicators such as heart rate, blood pressure and glucose levels and send real-time data to cloud-based platforms via secure wireless networks.[2] This enables healthcare personnel to remotely monitor patient states and anticipate issues, allowing for prompt interventions.[3] Smart cardiac pacemakers and defibrillators detect arrhythmias or malfunctions and immediately warn doctors, significantly reducing life-threatening risks.[4] Similarly, IoT-enabled orthopaedic implants, such as connected hip and knee replacements, track mechanical strain, joint movement and degeneration, providing important information about implant longevity and efficacy. These insights enable surgeons to spot early signs of failure, allowing for timely medical intervention and improving long-term patient outcomes.[5] Furthermore, advances in IoT have permitted robotic-assisted operations, increasing implant placement precision through AI-integrated devices that provide real-time feedback during treatments.[6] This is especially useful in delicate treatments like orthopaedic or dental surgery, where precise alignment and placement are required.

Another ground-breaking innovation is drug-delivery implants that provide medication in regulated doses customised to individual patient needs. IoT-enabled insulin pumps continually monitor glucose levels and dispense appropriate insulin dosages, improving treatment adherence and lowering complications for patients with chronic diseases like diabetes.[7] These modern technologies not only improve therapeutic efficacy, but they also reduce the possibility of human error in pharmaceutical delivery.[8] Furthermore, IoT devices linked with implants allow for self-diagnosis by detecting flaws such as battery depletion or structural damage and sending notifications to patients and clinicians.[8] This proactive

technique ensures early maintenance, improves implant durability and increases patient safety.[7]

Despite the significant advancements that IoT has enabled in implant operations, data security, privacy and ethical adherence remain critical challenges. The constant collecting and transmission of sensitive health data puts patients at risk of cyberattacks and unauthorised access.[9] Implementing strong encryption, cybersecurity safeguards and complete data protection is critical for safeguarding patient information.[9] Furthermore, healthcare systems must adhere to high regulatory standards to ensure the safety and efficacy of IoT-enabled implants, while also encouraging transparency about data usage and patient consent. Ethical considerations, such as informed patient permission and faith in technology, are critical to the adoption and effectiveness of IoT-based solutions.

Brain computer interface technology plays a crucial role in enhancing the diagnosis, treatment and rehabilitation of neurological conditions, thereby improving patients' quality of life and advancing neurotechnology.[10] Furthermore, the recent integration of the IoT in healthcare, particularly for implants, has transformed patient care by enabling real-time data collection and sophisticated analytics. IoT-enabled implants facilitate proactive and individualised post-surgical management through continuous health monitoring, providing healthcare providers with valuable insights into recovery and allowing for timely intervention, thus minimising complications.[11] The subsequent sections examine the advantages of IoT implant-based surgeries, including improved patient monitoring, tailored rehabilitation and predictive analytics, while also addressing potential risks, such as security concerns, biocompatibility issues and ethical and legal considerations.

Benefits and risks of IoT implant-based surgery

IoT-enabled implants in surgery offer transformative benefits for patient care and medical advancement by enabling the continuous monitoring of patient health metrics, which allows for precise and timely interventions.[12] For example, IoT sensors integrated into rehabilitation programs can track patient movement and progress, streamline clinical decision-making and reduce the workload of human caregivers.[12] In epilepsy management, IoT-based seizure monitoring systems enhance patient's quality of life by allowing remote monitoring and timely detection of seizures, providing added safety and convenience.[13]

However, integrating the IoT into medical implants introduces significant security and privacy risks. Large-scale IoT networks create vulnerabilities, as a lack of standardised security protocols opens the door to cyber-attacks.[14] This concern is particularly critical in healthcare, where the sensitivity of patient data is of paramount importance. Malicious actors can exploit IoT devices, potentially forming botnets to launch large-scale attacks, such as Distributed Denial-of-Service (DDoS), which threaten the integrity and availability of medical systems.[15]

Researchers have investigated advanced security solutions to mitigate these risks. Post-Quantum Cryptography (PQC) is one such solution under exploration that offers future-ready protection for IoT-based health devices against quantum computing threats.[16] Additionally, emerging energy-based attack detection methods provide a promising approach for identifying security breaches in IoT devices by detecting abnormal power consumption patterns.[14] Blockchain-based Intrusion Detection Systems (IDS) are also gaining attention because of their potential to create a decentralised, secure platform that facilitates global collaboration to tackle IoT security issues in healthcare.[17] As IoT technology continues to advance, a balanced approach that combines the benefits of improved patient care with robust security measures is essential for successful implementation of IoT-enabled implants in surgery.

Improving surgical outcomes through IoT vs ethical and regulatory dimensions

The integration of IoT technologies in healthcare, particularly in surgical settings, offers significant potential for improving outcomes, while simultaneously raising important ethical and regulatory considerations. IoT devices and sensors can transform surgical procedures through real-time monitoring, data collection and analysis. These technologies enable continuous tracking of patient vital signs, equipment status and environmental conditions in operating rooms.[18] The ability to gather and analyse vast amounts of data can lead to more informed decision making, enhanced patient safety and optimised resource allocation.[19] Furthermore, IoT integration can

facilitate remote patient monitoring and reduce hospitalisation rates, potentially decreasing hospital stay and improving overall patient care.[18]

However, the implementation of the IoT in surgical settings presents significant ethical and regulatory challenges. Data privacy and security are paramount concerns because the sensitive nature of medical information necessitates robust protection measures.[18, 20] The utilisation of AI and machine-learning algorithms in conjunction with IoT devices raises questions regarding algorithmic bias, transparency and accountability in decision-making processes. Furthermore, the rapid advancement of these technologies frequently outpaces the existing regulatory frameworks, necessitating the development of new legislation and guidelines to ensure ethical use and patient protection.

In conclusion, although IoT technologies offer significant potential for improving surgical outcomes through enhanced monitoring, data analysis and decision support, their implementation must be carefully balanced with ethical considerations and regulatory compliance. Implant operations have improved precision, real-time diagnostics, remote monitoring and early problem detection through the IoT. Intelligent implants improve outcomes, recovery and long-term health management. AI-assisted robotic surgeries, real-time analytics and drug-delivery devices improve surgical and postoperative care. Innovation and strict data privacy, cybersecurity and ethical compliance are needed to realise IoT's healthcare potential. Addressing these issues will provide safer, smarter and more reliable IoT-enabled implants, improving patient safety, clinical outcomes and healthcare overall.

Ethics

No ethics approval was required, since the form of this article is a letter to the editor, expressing authors' personal views.

Data access

The data that support the findings of this study are available from the corresponding author upon reasonable individual request.

Acknowledgement

Authors are thankful to their parent institutions for the facilities.

Author ORCID numbers

Praveen Ramakrishnan (PR):
0000-0003-4644-1189
Abdulkadhar Mohamed Jalaludeen (AMJ):
0000-0002-3633-020X
Lalitha Gnansekaran (LG):
0009-0005-1560-2965
Thanigaivel Sundaram (TS):
0000-0002-8698-3858
Shivani Chopra (SC):
0000-0002-5890-389X
Hitesh Chopra (HC):
0000-0001-8867-7603

Conflicts of interest

The authors declare that there is no conflict of interest.

Funding

The authors received no funding to support the publication of this article.

Author contributions

Conceptualisation: PR, AMJ
Data curation: LG, TS
Writing - original draft: PR, AMJ, LG, TS
Writing - review and editing: SC, HC
Project administration: SC, HC

References

1. Adeoye S, Adams R. Revolutionizing healthcare: the impact and future of the Internet of Things (IoT) in the Health Sector. Cognizance J Multidisc Stud. 2024;4(10):127–43. doi: 10.47760/cognizance.2024.v04i10.009.
2. Thangam S, Niranjan DK, Shyam KM, Kumar ReddyMC, Aravind A, SaiIo T. Based health monitoring system for forbidden patients. In: 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2024; pp. 1155–63. doi: 10.1109/ICACCS60874.2024.10717190.
3. Raymond DA, Apetorgbor M, Kumar P, Goureshettiwar P. IoT-enabled smart implants: revolutionizing post-surgical care. In: 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), IEEE, 2024; pp. 430–5. doi: 10.1109/ICSCSS60660.2024.10625029.
4. Odirichukwu JC, Eze EO, Eze VC, Eze EI, Njoku OA, Chika-Ugada PK, et al. Internet of Things (IoT) based patient information and heart beat monitoring system for health information system. J Firewall Softw Netw 2024;2(1):20–8. doi: 10.48001/jofsn.2024.2120-28.
5. Khatib IA, Shamayleh A, Ndiaye M. Healthcare and the Internet of medical things: applications, trends, key challenges, and proposed resolutions. Informatics. 2024;11(3):47. doi: 10.3390/informatics11030047.
6. [Rashid M. Artificial Intelligence in surgery: transforming the future of operative care. Develop Med Life Sci. 2024;1(3):1–4. doi: 10.69750/dmls.01.03.034.
7. Chappel E. Implantable drug delivery devices. In: ChapeL E, ed. Drug delivery devices and therapeutic systems. Amesterdam: Elsevier 2021; pp. 129–156. doi: 10.1016/B978-0-12-819838-4.00001-8.
8. Zhang J, Xu J, Lim J, Nolan JK, Lee H, Lee CH. Wearable glucose monitoring and implantable drug delivery systems for diabetes management. Adv Healthc Mater. 2021 Sep;10(17):e2100194. doi: 10.1002/adhm.202100194.
9. Verma V, Mishra A, Bisht V, Bala J. Internet of diagnostic things: emerging horizon towards precision and digital health care. J Health Sci Res. 2020;5(2):51–61. doi: 10.7324/jhsr/2020/24981.
10. Zhang H, Jiao L, Yang S, Li H, Jiang X, Feng J, et al. Brain-computer interfaces: the innovative key to unlocking neurological conditions. Int J Surg. 2024 Sep 1;110(9):5745-62.doi:10.1097/JS9.0000000000002022.
11. Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MAM, Bairagi AK, Khan MA, et al. IoT-based healthcare-monitoring system towards improving quality of life: a review. Healthcare (Basel). 2022 Oct 11;10(10):1993. doi: 10.3390/healthcare10101993.
12. Aziz R, Sundus H, Jawed F, Khan SA. Wearable IoT devices in rehabilitation. In: Medical robotics and AI-assisted diagnostics for a high-tech healthcare Industry. Hershey, PA, USA: IGI-Global, 2024; doi: 10.4018/979-8-3693-2105-8.ch018.
13. Patro KK, Prakash AJ, Sahoo JP, Routray S, Baihan A, Samee NA, et al. SMARTSeiz: Deep learning with attention mechanism for accurate seizure recognition in IoT healthcare devices. IEEE J Biomed Health Inform. 2024 Jul;28(7):3810-8. doi: 10.1109/JBHI.2023.3336935.
14. erlino V, Allegra D. Energy-based approach for attack detection in IoT devices: A survey. Internet Things 2024;27: 101306. doi: 10.1016/j.iot.2024.101306.
15. Gelgi M, Guan Y, Arunachala S, Samba Siva Rao M, Dragoni N. Systematic literature review of IoT Botnet DDOS attacks and evaluation of detection techniques. Sensors (Basel). 2024 Jun 1;24(11):3571. doi: 10.3390/s24113571.
16. Mansoor K, Afzal M, Iqbal W, Abbas Y, Mussiraliyeva S, Chehri A. PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. Internet Things. 2024;27: 101228. doi: 10.1016/j.iot.2024.101228.
17. Hızal S, Akhter AFMS, Çavuşoğlu 101228, Akgün D. Blockchain-based IoT security solutions for IDS research centers, Internet Things. 2024;27:101307. doi: 10.1016/j.iot.2024.101307.
18. Singiri S, Katari SC, Reddy Vootukuri NG. Security protocols in healthcare: A comprehensive study of AI-Enabled IoMT. Magna Sci Adv Biol Pharm. 2024;12(1):32-7. doi: 10.30574/msabp.2024.12.1.0030.
19. Althoey F, Waqar A, Hamed Alsulamy S, Khan AM, Alshehri A, Idris Falqi I, et al. Influence of IoT implementation on Resource management in construction. Heliyon. 2024 May 31;10(15):e32193. doi: 10.1016/j.heliyon.2024.e32193.
20. Halgamuge MN, Niyato D. Adaptive edge security framework for dynamic IoT security policies in diverse environments, Comput Sec. 2024;148: 104128. doi: 10.1016/j.cose.2024.104128.