STM JOURNALS

International Journal of
Mobile Computing Technology

Volume 2, Issue 1, 2024
January—June
DOI (Journal): 10.37591/IJMCT

https://journals.stmjournals.com/ijmct

Review IJMCT

Biomedical Monitoring, IoT in Hospital Industry: Focusing on Solidification of Data Security and Privacy of Patients

Bhupinder Singh*

Abstract

Improving the security of internet of things (IoT) communication and ensuring the safety of intelligent healthcare systems are significant objectives for biomedical microelectromechanical systems (BioMEMS). BioMEMS, which are at the cusp of healthcare and cutting-edge technology, propel the creation of tailored monitoring, therapeutics, and diagnostics. But because of the intricate security and privacy issues that come with IoT connections in smart healthcare ecosystems, a careful analysis is required. Various security solutions are explored, including robust authentication processes, data encryption, resistant design against attacks, and continuous monitoring mechanisms, all tailored to bolster BioMEMS against evolving threats in smart healthcare environments. This paper underscores the significance of ethical and regulatory considerations, advocating for patient autonomy, data confidentiality, and equitable healthcare access in the context of IoT communication security This paper addresses risks such as cyberattacks, data manipulation, and communication interception by doing a thorough examination of the complex security landscape surrounding IoT communications in BioMEMS.

Keywords: Biomedical monitoring, hospital industry, internet of things (IoT), data, privacy, patient information

INTRODUCTION

Healthcare organizations place a high value on health information systems (HISs) because of their ability to exchange patient health information in a seamless manner, securely store it, retrieve it quickly, analyze it analytically, and share it collectively [1]. These systems are designed to meet the requirements of patients while protecting the privacy and security of medical data [2]. They cover elements such as availability, confidentiality, and integrity, all of which are essential for providing high-quality healthcare services [3]. This paper looks at several technologies and approaches that are presently being used to improve the security and privacy of medical data inside HISs through a thorough analysis of the literature [4]. Cloud computing, blockchain, mobile health apps, internet of things (IoT), and hybrid solutions are just a few of the technologies that have been used to improve the security of medical data [5]. HISs are all-inclusive technology platforms designed to organize and manage data and information about health [6]. They support clinical decision-making and enhance patient care and outcomes by helping healthcare organizations store, retrieve, analyze, and share patient health information [7]. HISs usually encompass various software tools and applications designed for clinical decision support (CDS), electronic health records (EHRs), health information exchange, and administrative tasks [8]. These flexible systems may

***Author for Correspondence**
Bhupinder Singh
E-mail: bhupindersinghlaw19@gmail.com

Professor, School of Law, Sharda University, Greater Noida, Uttar Pradesh, India

Received Date: April 11, 2024
Accepted Date: April 20, 2024
Published Date: May 9, 2024

Citation: Bhupinder Singh. Biomedical Monitoring, IoT in Hospital Industry: Focusing on Solidification of Data Security and Privacy of Patients. International Journal of Mobile Computing Technology. 2024; 2(1): 26–29p.

be used in a variety of contexts, including clinics, long-term care homes, public health organizations, and even homes. Additionally, HISs ensure data security and privacy by adhering to regulations like the Health Insurance Portability and Accountability Act (HIPAA) [9].

BIOMEDICAL MONITORING, IoT IN HOSPITAL INDUSTRY

The healthcare industry has experienced a substantial evolution due to the integration of IoT technology, leading to inventive solutions that improve patient care, streamline operations, and enable remote monitoring [10]. IoT in healthcare entails an interconnected system of medical devices, sensors, wearables, and other technologies that gather and relay data in real-time, offering valuable insights into patient health status, vital signs, medication compliance, and potential health hazards [11]. Remote patient monitoring, telemedicine solutions, smart wearables, smart healthcare solutions, and linked medical equipment are five essential uses of IoT in healthcare [12]. These apps provide enhanced patient safety through precise data transfer and prompt interventions, as well as remote vital sign monitoring, virtual consultations, tracking of health indicators, asset tracking, and inventory management [13]. IoT technology has many advantages for the healthcare industry, but there are drawbacks as well that must be considered [14]. The volume of sensitive patient data that is gathered and sent via IoT devices raises data security and privacy issues, emphasizing the necessity of strong security measures and encryption techniques [15]. The broad use of IoT in healthcare is hindered by a number of factors, including ethical concerns about patient privacy and data exploitation, lack of legal framework, interoperability difficulties, and the accuracy and dependability of IoT devices [16]. To guarantee the appropriate and ethical use of IoT technology in patient care, addressing these difficulties necessitates extensive examination, validation, and implementation of regulatory frameworks and ethical norms [17].

SOLIDIFICATION OF DATA SECURITY AND PRIVACY OF PATIENTS

The rise of digitalization in patient health information, particularly through EHRs and personal health records, presents fresh and significant challenges to the security and privacy of patient data [18]. Medical data breaches can affect sensitive information regarding a patient's health and personal life, such as diagnosis, treatments, medical history, and personal identifiers [19, 20]. Serious repercussions from such breaches include identity theft, fraud, and medical blunders [21]. Ensuring patient data security is essential for fostering people's willingness to share their personal health information for present or future healthcare needs [22, 23]. In addition, healthcare providers could be reluctant to capture complete patient data if they do not trust that the organization would protect their records [24]. Privacy and security concerns must be given top priority in HISs [25]. This entails using safe technology to transmit and store data, putting strong access restrictions in place, and educating medical staff members on the best ways to protect patient privacy and security [26]. Moreover, the delivery of superior healthcare services hinges on upholding the security and confidentiality of medical data, encompassing aspects such as availability, confidentiality, and integrity [27]. Because of their similar language, medical IoT, healthcare IoT, and biomedical IoT are sometimes confused, creating misunderstandings regarding their interchangeability. The healthcare IoT often refers to processes, including procedures, tests, diagnoses, and treatments, however the lines separating them are not always obvious [28]. On the other hand, because they both include platforms, tools, hardware, and software, Medical IoT and biomedical IoT are frequently used synonymously. We shall refer to these systems and technologies as "medical IoT" throughout [29].

CONCLUSION

The acceptance and efficacy of IoT devices in healthcare settings are significantly influenced by their usability and user-friendliness. The potential advantages of IoT in healthcare might be limited if these systems and gadgets prove to be too complicated or difficult for patients and healthcare professionals to incorporate into their regular routines. This could hinder their acceptability. The IoT has enormous promise to change healthcare, despite these challenges. The continuous advancements and enhancements in IoT technology hold promise for transforming healthcare delivery, enhancing patient outcomes, and elevating overall standards of care. The healthcare sector may take a more patient-centric

and effective approach to providing healthcare services by integrating smart devices, real-time data processing, and remote monitoring capabilities. In summary, IoT has become a key factor in changing the healthcare environment. Connectivity, immediate data gathering, and analytical capabilities have unlocked a realm of opportunities to enhance patient care, increase efficiency, and fundamentally alter healthcare delivery. Healthcare companies may fully realize the promise of IoT technology to develop a more efficient, customized, and safe healthcare system by adopting it and resolving related issues.

REFERENCES

1. Mathkor DM, Mathkor N, Bassfar Z, Bantun F, Slama P, Ahmad F, Haque S. Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: an overview of current and future innovative trends. J Infect Public Health. 2024; 17 (4): 559–572.
2. Sudha K, Balakrishnan C, Varun CM, Subramanian RS. Advancements in medical robotics and AI-assisted diagnostics: transforming the healthcare industry. In: Khang A, editor. AI-Driven Innovations in Digital Healthcare: Emerging Trends, Challenges, and Applications. Hershey, PA, USA: IGI Global; 2024. pp. 23–46.
3. Singh B, Kaunert C, Vig K. Reinventing influence of artificial intelligence (AI) on digital consumer lensing transforming consumer recommendation model: exploring stimulus artificial intelligence on consumer shopping decisions. In: Musiolik TH, Rodriguez RV, Kannan H, editors. AI Impacts in Digital Consumer Behavior. Hershey, PA, USA: IGI Global; 2024. pp. 141–169.
4. Khang A, editor. Medical Robotics and AI-Assisted Diagnostics for a High-Tech Healthcare Industry. Hershey, PA, USA: IGI Global; 2024.
5. Nalluri M, Rongali AS, Pulimamidi R, Babu Mupparaju C. Autonomous health monitoring and assistance systems using IoT. Pak Heart J. 2024; 57 (1): 52–60.
6. Singh B. Featuring consumer choices of consumable products for health benefits: evolving issues from tort and product liabilities. J Law Torts Consumer Protect Law. 2024; 7 (1): 53–56.
7. Karmakar S, Mishra A, Mishra AK, Srivastava JP. Robotics in medical science. In: Srivastava JP, Kozak D, Ranjan V, Kumar P, Kumar R, Tayal S, editors. Mechanical Engineering in Biomedical Applications: Bio-3D Printing, Biofluid Mechanics, Implant Design, Biomaterials, Computational Biomechanics, Tissue Mechanics. New York, NY, USA: Wiley; 2024. pp. 367–396.
8. Singh B. Unleashing alternative dispute resolution (ADR) in resolving complex legal-technical issues arising in cyberspace lensing e-commerce and intellectual property: proliferation of e-commerce digital economy. Revista Brasileira de Alternative Dispute Resolution – Brazilian Journal of Alternative Dispute Resolution. 2023; 5 (10): 81–105.
9. Singh B, Kaunert C. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. GLS Law J. 2024; 6 (1): 13–20.
10. Singh B. Green infrastructure in real estate landscapes: pillars of sustainable development and vision for tomorrow. Natl J Real Estate Law. 2024; 7 (1): 4–8.
11. Singh B. Telehealth monitoring lensing deep neural learning structure: ambient patient wellness via wearable devices for real-time alerts and interventions. Indian J Health Med Law. 2023; 6 (2): 32–36.
12. Singh B. Cherish growth, advancement and tax structure: addressing social and economic prospects. J Tax Regul Framework. 2024; 7 (1): 7–10.
13. Sachdeva S, Bhatia S, Al Harrasi A, Shah YA, Anwer K, Philip AK, Shah SF, Khan A, Halim SA. Unraveling the role of cloud computing in health care system and biomedical sciences. Heliyon. 2024; 10 (7): e29044.
14. Singh B. Legal dynamics lensing metaverse crafted for videogame industry and e-sports: phenomenological exploration catalyst complexity and future. J Intellect Property Rights Law. 2024; 7 (1): 8–14.
15. Talpur MS, Abro AA, Ebrahim M, Kandhro IA, Manickam S, Arfeen SU, Dandoush A, Uddin M. Illuminating healthcare management: a comprehensive review of IoT-enabled chronic disease monitoring. IEEE Access. 2024; 12: 48189–48209.

16. Singh B. Blockchain technology in renovating healthcare: legal and future perspectives. In: Kaushik K, Dahiya S, Aggarwal S, Dwivedi AD, editors. Revolutionizing Healthcare Through Artificial Intelligence and Internet of Things Applications. Hershey, PA, USA: IGI Global; 2023. pp. 177–186.
17. Rao TV, Mothukuri L, Bhavana S. IoT networks for real-time healthcare monitoring systems. In: Baral SK, Goel R, editors. Analyzing Current Digital Healthcare Trends Using Social Networks. Hershey, PA, USA: IGI Global; 2024. pp. 143–158.
18. Singh B. Federated learning for envision future trajectory smart transport system for climate preservation and smart green planet: insights into global governance and SDG-9 (industry, innovation and infrastructure). Natl J Environ Law. 2023; 6 (2): 6–17.
19. Sharma A, Singh B. Measuring impact of e-commerce on small scale business: a systematic review. J Corporate Govern Int Business Law. 2022; 5 (1): 34–38.
20. Barua R, Datta S. The ongoing advancements in surgical robotics: transforming the landscape of surgery. In: Khang A, editor. AI-Driven Innovations in Digital Healthcare: Emerging Trends, Challenges, and Applications. Hershey, PA, USA: IGI Global; 2024. pp. 288–303.
21. Singh B. Understanding legal frameworks concerning transgender healthcare in the age of dynamism. Electron J Soc Strategic Stud. 2022; 3: 56–65.
22. Ness S, Xuan TR, Oguntibeju OO. Influence of AI: robotics in healthcare. Asian J Res Computer Sci. 2024; 17 (5): 222–237.
23. Singh B. Relevance of agriculture-nutrition linkage for human healthcare: a conceptual legal framework of implication and pathways. Justice Law Bull. 2022; 1 (1): 44–49.
24. Afreen H, Amir A, Farooq U. An IoT-assisted patient monitoring and alert system. J Comput Biomed Inform. 2024; Article 004-SI.
25. Singh B. COVID-19 pandemic and public healthcare: Endless downward spiral or solution via rapid legal and health services implementation with patient monitoring program. Justice Law Bull. 2022; 1 (1): 1–7.
26. Singh B. Global science and jurisprudential approach concerning healthcare and illness. Indian J Health Med Law. 2020; 3 (1): 7–13.
27. Sharmila EMN, Rama Krishna K, Prasad GNR, Anand B, Kwatra CV, Kapila D. IoMT—applications, benefits, and future challenges in the healthcare domain. In: Yadav SP, Yadav S, Raj P, de Albuquerque VHC, editors. Advances in Fuzzy-Based Internet of Medical Things (IoMT). New York, NY, USA: Wiley; 2024. pp. 1–23.
28. Singh B. Profiling public healthcare: a comparative analysis based on the multidimensional healthcare management and legal approach. Indian J Health Med Law. 2019; 2 (2): 1–5.
29. Tettey F, Parupelli SK, Desai S. A review of biomedical devices: classification, regulatory guidelines, human factors, software as a medical device, and cybersecurity. Biomed Mater Devices. 2024; 2 (1): 316–341.

