

Chapter 16

The Ethics of AI and IoT in Healthcare: Navigating Cybersecurity Risks and Ensuring Data Protection

Sagar Sidana

 <https://orcid.org/0009-0007-8399-0247>

Maharshi Dayanand University, India

Parul Chaudhary

 <https://orcid.org/0000-0002-4787-0244>

Maharaja Surajmal Institute of Technology, India


Amrita Ticku

Bharti Vidyapeeth's College of Engineering, New Delhi, India

Nitasha Rathore

Bharati Vidyapeeth's College of Engineering, New Delhi, India


Anurag Sinha

 <https://orcid.org/0000-0002-1034>

-6334

School of Computing and Information Science, IGNOU, New Delhi, India

Ashutosh Keshri

 <https://orcid.org/0009-0008-7672-8360>

Amity University, Ranchi, India

Biresh Kumar

Amity University, Ranchi, India

Neetu Singh

Bharati Vidyapeeth's College of Engineering, New Delhi, India

Abhiraj Sinha

BIT Mesra, India

Neeraj Raj

Independent Researcher, India

ABSTRACT

The integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies in healthcare has revolutionized patient care by enabling advanced monitoring,

DOI: 10.4018/979-8-3693-4147-6.ch016

Copyright © 2025, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

personalized treatments, and real-time data analysis. However, this technological advancement also brings to the forefront significant ethical and cybersecurity challenges. This paper explores the delicate balance between the benefits of AI and IoT in healthcare and the associated risks to patient data security. We examine the ethical implications of deploying AI-driven IoT devices, focusing on issues such as data privacy, consent, and the potential for unintended consequences. Additionally, we address the cybersecurity vulnerabilities inherent in IoT devices, including risks of data breaches and unauthorized access. By analyzing current strategies and proposing frameworks for enhancing data protection.

I. INTRODUCTION

The advent of Artificial Intelligence (AI) and Internet of Things (IoT) technologies has significantly transformed the landscape of healthcare, offering unprecedented opportunities for improving patient care, diagnostics, and treatment outcomes. AI-powered IoT devices, such as wearable health monitors and smart medical equipment, enable continuous data collection, real-time monitoring, and personalized medical interventions. These innovations hold the promise of enhancing healthcare efficiency, reducing costs, and tailoring treatments to individual patient needs. Despite these benefits, the integration of AI and IoT in healthcare introduces a complex array of ethical and cybersecurity challenges. The vast amounts of sensitive patient data generated and transmitted by these devices raise critical concerns about data privacy, security, and the potential for misuse. The interconnected nature of IoT systems creates numerous entry points for cyberattacks, posing risks such as data breaches, identity theft, and unauthorized access to personal health information.

Ethically, the deployment of AI and IoT in healthcare necessitates a careful examination of issues related to informed consent, data ownership, and the potential biases inherent in AI algorithms. The dynamic nature of these technologies further complicates the establishment of robust ethical guidelines and regulatory standards. This paper aims to explore the intersection of AI and IoT in healthcare, focusing on the ethical and cybersecurity implications associated with their use. We will analyze the risks and rewards of these technologies, evaluate current security measures, and propose strategies for safeguarding patient data while maximizing the benefits of AI and IoT innovations. By addressing these challenges, we seek to contribute to a framework that balances technological advancement with ethical responsibility and data protection. The Web of Things, also known as the Internet of Things (IoT), has become an integral part of our daily lives. These devices are employed in numerous settings to offer various services that simplify our routines. However, the rapid proliferation of IoT devices has raised significant security concerns. These devices

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/the-ethics-of-ai-and-iot-in-healthcare/359651

Related Content

Exploring Privacy Notification and Control Mechanisms for Proximity-Aware Tablets

Huiyuan Zhou, Vinicius Ferreira, Thamara Silva Alves, Bonnie MacKay, Kirstie Hawkey and Derek Reilly (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 227-247).

www.irma-international.org/chapter/exploring-privacy-notification-and-control-mechanisms-for-proximity-aware-tablets/228729

Legal Challenges and Policy Responses to Deepfake Abuse in Schools

R. Sivakani, Amit Kumar Kashyap, Rehana Parveen, Biranchi Narayan P. Panda, P. Paramasivanand R. Regin (2026). *Safeguarding Educational Integrity Through Deepfake Face Detection* (pp. 191-212).

www.irma-international.org/chapter/legal-challenges-and-policy-responses-to-deepfake-abuse-in-schools/398645

Privacy and Security: Safeguarding Personal Data in the AI Era

Geeta Sandeep Nadella, Hari Gonaygunta, Mohan Harishand Pawan Whig (2025). *Ethical Dimensions of AI Development* (pp. 157-174).

www.irma-international.org/chapter/privacy-and-security/359642

Sealing One's Online Wall Off From Outsiders: Determinants of the Use of Facebook's Privacy Settings Among Young Dutch Users

Ardion Beldad (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 854-869).

www.irma-international.org/chapter/sealing-ones-online-wall-off-from-outsiders/228759

Penetration Testing Tools and Techniques

Abhijeet Kumar (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 280-306).

www.irma-international.org/chapter/penetration-testing-tools-and-techniques/330269