Progress on Multidisciplinary Scientific Research and Innovation

"Volume 1, Issue 1, Year 2024"

website: https://www.c5k.com

Multidisciplinary Journal on Information Technology Management and Business Magazine
www.c5k.com

Research Article

Artificial Intelligence Based Healthcare: Applications, Challenges, and Future Directions

Tahmina Akther[1,*], Misha Billah[2], Md Samiun[3], Md. Firoz Hossain[4], Md Mesbah Uddin[5], Ishrat Jahan[6], Md Shawon Islam[7]

[1]*Department of Business Management, Monroe University, 1201 North Third Street Suite 7-300. Baton Rouge, LA 70802, USA*
[2]*Department of Mathematics, University of Texas at Dallas, 2811 North Floyd Road, Richardson, USA*
[3]*Department of Business Administration, International American University, #1000 Los Angeles, CA 90010, USA*
[4]*Institute of Social Welfare and Research, University of Dhaka, Shahbag, Dhaka 1205, Bangladesh.*
[5]*Department of Occupational and Environmental Health, Bangladesh University of Health Science, 125, Technical Mor, 1 Darus Salam Rd, Dhaka 1216*
[6]*Department of Information Security, ITMO University, Kronverkskiy Prospekt, 49, St Petersburg, Russia, 197101*
[7]*Department of Electrical & Electronic Engineering, Mymensingh Engineering College (University of Dhaka), Mymensingh-2208, Bangladesh*
**Corresponding Author:* takther9478@monroeu.edu

ARTICLE INFO

Article history:
01 Jul 2024 (Received)
10 Aug 2024 (Accepted)
18 Aug 2024 (Published Online)

Keywords:
AI-based Healthcare, Healthcare 5.0, IoT for Healthcare, Healthcare 4.0, Artificial Intelligence.

ABSTRACT

Healthcare services are being transformed by AI, IoT, big data analytics, blockchain, and cloud computing, transforming the medical model from disease-centered to patient-centered care. AI enables doctors to make more accurate diagnoses, health administrators to locate electronic health records faster, and patients to receive timely, personalized treatments. Healthcare 5.0, a comprehensive transformation, focuses on personalization and customer-centered care, aiming for lifelong partnership, customer well-being, and quality of life. However, security challenges such as managing large data volumes, lack of standards, data security threats, and regulatory difficulties persist. A robust security framework is needed to secure the data of Healthcare 5.0, facilitating authentication, access control, key management, and intrusion detection. This review article proposes the design of a secure generalized healthcare 5.0 framework, detailing various applications, security requirements, threat models, existing security mechanisms, and future research directions for researchers working in this domain.

DOI: https://doi.org/10.63471/pmsri24003 @ 2024 Progress on Multidisciplinary Scientific Research and Innovation (PMSRI), C5K Research Publication

1. Introduction

AI is revolutionizing healthcare by performing tasks typically performed by humans in less time and cost. It enhances patient experiences, improves resource management, and enables accurate diagnoses. Healthcare 5.0, a comprehensive transformation utilizing IoT, AI, big data analytics, blockchain, and cloud computing, aims to shift the medical model from disease-centered to patient-centered care(Saraswat et al., 2022). Healthcare 1.0 focused on production, while Healthcare 2.0 focused on industrializing and value chain, while Healthcare 3.0 focused on automation and operating models. Healthcare 4.0 shifted to the business model, focusing on uniqueness, mass personalization, and proactive healthcare. Currently, healthcare 5.0 focuses on personalization and customer-centered care, aiming for lifelong partnership, customer well-being, and quality of life(Deepti Saraswat, 2022; Poonam Rani, 2022).

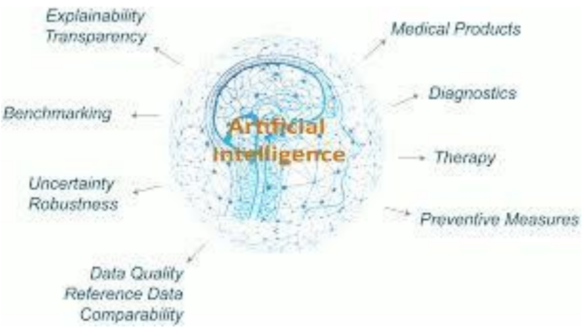

Fig. 1. Use of AI for healthcare.

However, healthcare 5.0 faces security challenges such as managing large data volumes, lack of standards, data security threats, and regulatory difficulties. Different information security-related attacks, such as replay, man-in-the-middle (MiTM), impersonation, malware injection, and Denial-of-Service (DoS), can compromise sensitive healthcare data. Therefore, a

*Corresponding author: takther9478@monroeu.edu (Tahmina Akther)

Cite: Tahmina Akther, Misha Billah, Md Samiun, Md. Firoz Hossain, Md Mesbah Uddin, Ishrat Jahan, Md Shawon Islam (2024). Artificial Intelligence Based Healthcare: Applications, Challenges, and Future Directions. *Progress on Multidisciplinary Scientific Research and Innovation,* 1(1), pp. 7-11.

robust security framework is needed to secure the data of Healthcare 5.0.

This review article discusses various applications of AI-based healthcare, primarily relevant to Healthcare 5.0, security requirements, threats, attacks, and a generalized secure Healthcare 5.0 framework. It also provides a detailed comparative study among existing security schemes in Healthcare 4.0 and Healthcare 5.0. The paper concludes by highlighting the importance of a robust security framework for Healthcare 5.0.

2. Literature review

The term artificial intelligence (AI) was initially used in 1950, but its general adoption and use in medicine was hindered by several flaws in the initial models. With the introduction of deep learning in the early 2000s, many of these restrictions were removed. We are entering a new era in medicine where AI may be used in clinical practice through risk assessment models, increasing workflow efficiency and diagnostic accuracy. AI systems are now able to analyze complicated algorithms and learn on their own. This article provides a quick historical overview of artificial intelligence's progress over the last few decades as well as its current introduction and advancement in the field of medicine(Vivek Kaul, 2020).

The paper, Blockchain-based IoT enabled health monitoring system, proposes a secure four-layer IoT-enabled health monitoring system that collects patient data and classifies it into medical categories using transfer learning, shown in Fig. 2. The framework uses blockchain for security and incorporates transfer learning to use multiple pre-trained models. The routing technique uses factors like probability, credibility rating, and node energy to reduce network overhead and energy use. The system classifies patient information using four pre-trained convolutional neural network models: ResNet50, VGG19, InceptionV3, and SqueezeNet. Simulations show a 92.24% classification accuracy, demonstrating the potential of this secure architecture in health monitoring systems(Poonam Rani, 2022).

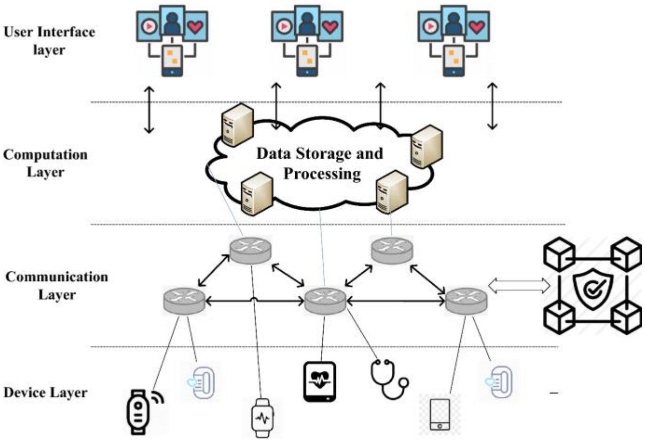

Fig. 2. Blockchain-based IoT-enabled health monitoring system.

IoT technology is revolutionizing health care by enabling wireless, interconnected devices to collect, send, and store data, enhancing service delivery and predicting health issues. Government leaders worldwide are implementing policies to deliver healthcare services using technology, especially in response to the COVID-19 pandemic. IoT-based health care can improve the accessibility of preventative public health services and transition secondary and tertiary healthcare to a more proactive, continuous, and coordinated system. However, potential issues include barriers to market adoption, privacy, security, interoperability, standardization, data storage, and control(Jaimon T Kelly, 2020).

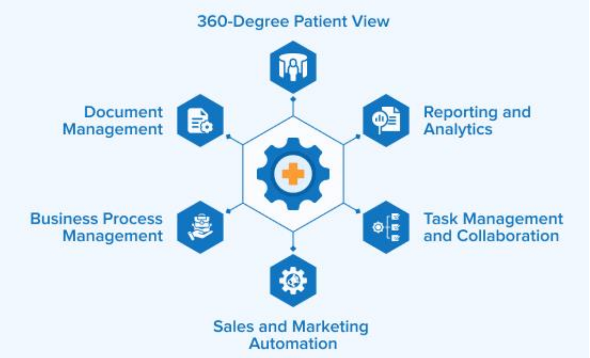
360-Degree Patient View
Document Management
Reporting and Analytics
Business Process Management
Task Management and Collaboration
Sales and Marketing Automation

Fig. 3. Features of Healthcare 5.0 CRM software.

The paper, Sensors, and Healthcare 5.0 (Fig. 3), represents that Healthcare 5.0 is a paradigm shift towards smart disease control, virtual care, smart health management, smart monitoring, and decision-making. Emerging technologies like nanotechnology, 5G, drone technology, blockchain, robotics, big data, the Internet of Things, artificial intelligence, and cloud computing are transforming healthcare. These technologies offer personalized monitoring, remote monitoring, and virtual clinics. However, challenges such as organizational challenges, technological and infrastructural barriers, lack of legal and regulatory frameworks, individual perceptions, funding, and religious and cultural barriers remain. To successfully implement Healthcare 5.0, there is a need to expand technological infrastructure, develop legal and e-health policies, and improve stakeholder engagement(Elliot Mbunge, 2021).

3. Applications of AI-based Healthcare

AI-based Healthcare offers important applications in various facilities and services, enhancing the efficiency and effectiveness of healthcare systems.

i. OPERATIONS MANAGEMENT IN HOSPITALS

Healthcare 5.0 is a revolutionary approach to hospital operations management, focusing on funding, personnel, policy development, equipment maintenance, and health insurance management. It addresses bottlenecks, enhances patient satisfaction, and improves service quality through smart medical devices.

ii. PATIENT REMOTE MONITORING

Healthcare 5.0 utilizes IoT and technologies for remote patient monitoring, improving services for elderly, disabled, and rural patients. Drone-based sample collection and smart devices assess health factors, reducing hospitalization and travel costs.

iii. DISEASE DETECTION AND TREATMENT

Healthcare 5.0 is a revolutionary approach to disease detection, assessment, and medication, utilizing smart devices and machine learning algorithms to monitor vital signs, enabling early detection of serious illnesses and prompt treatment.

iv. REMOTE SURGERY AND DRUGS

Healthcare 5.0 technologies enable remote surgery, real-time action, and improved drug supply chain management. Smart tags protect against counterfeiting and drone-based drug supply ensure high-quality prescriptions. Widely adopted, these technologies ensure accurate, reliable remote surgery, preserving lives during wars or disasters.

3.1. SECURITY REQUIREMENTS OF HEALTHCARE 5.0

Healthcare 5.0 Security and Privacy Requirements follows

→ Confidentiality: Protects against data release attacks, including data transmission and storage secrecy. Data encryption is used to ensure confidentiality.

→ Integrity: Ensures data integrity, preventing unapproved updates and data addition or removal without permission. Secure hash algorithms like SHA-256 are used.

→ Authentication: Determines the legitimacy of a person or object, involving device-to-device, user-to-device, or user-to-user authentication. Mechanisms like the two-factor user authentication protocol or the three-factor user authentication protocol are used.

→ Access control: Mitigates unauthorized access attempts to legitimate devices and resources. Mechanisms include device access control and user access control.

→ Non-repudiation: Ensures the integrity and evidence of the data origin of the transferred communications.

→ Authorization: Ensures genuine parties deliver the data to other parties.

→ Freshness: Ensures messages are fresh to reduce re-transmission tries.

→ Availability: Ensures devices and network services are accessible to real entities even in the worst circumstances.

→ Forward and Backward Secrecy: Ensures messages are kept confidential.

3.2. Healthcare 5.0 Potential Dangers and Attacks

→ Man-in-the-middle (MiTM) Attack: The adversary intercepts communications being sent and attempts to amend or delete them before sending them to the addressee.

→ Denial-of-Service (DoS) Attack: The adversary prevents authorised users from using the services of healthcare 5.0 by setting up an attacker system that delivers bogus requests or attack packets to legitimate healthcare 5.0 devices or services.

→ Attacks associated with Blockchain: The system consists of blockchain, which can be exploited by malicious miners A.

→ Database Attack: Healthcare 5.0 stores healthcare information on a server or cloud server, which can be exposed through SQL injection attack and Cross-Site Scripting (XSS) attack.

→ Physical Device Stolen Attack: The adversary can use stolen healthcare devices to extract confidential material and execute additional attacks like MiTM, illegal session key computation, impersonation attacks, etc.

→ Privileged-insider Attack: The registration authority's privileged insider user may pose as an A and use the obtained registration information to execute prospective attacks on healthcare 5.0.

→ Managing Large Data Volumes: Traditional mechanisms and algorithms struggle to process large volumes of medical data exchanged over healthcare 5.0. Machine learning and sophisticated algorithms could be a potential solution to manage this data.

→ Absence of Standards: Incompatibility of systems due to different types of smart healthcare devices can pose security and stability risks. Regular checks for devices used for data access are recommended.

→ Data Security Threats: Cyber attacks can compromise healthcare data, especially when more devices are connected to external systems.

→ Data Unification: Healthcare 5.0 devices must be compatible with each other to enable data transmission to all users, including payers and healthcare service providers.

→ Regulatory Difficulties: Different countries have different laws related to the privacy of sensitive healthcare data. Clinical-grade medical devices must have clearance from national regulatory authorities before market launch.

→ Cost Factor: Initial investment in hardware, specialized healthcare 5.0 infrastructure, cloud computing, and developing a consumer-facing app is high, but the return on investment is substantial.

3.3. HEALTHCARE 5.0 FRAMEWORK

The proposed secure healthcare 5.0 framework uses implantable and wearable medical devices to monitor patients' health, providing remote prescriptions and data analytics, shown in Fig. 4. During the pandemic, medical drones collect samples and deliver medicines. However, health-related data exchange is vulnerable to security attacks like replay, man-in-the-middle, and malware injection.

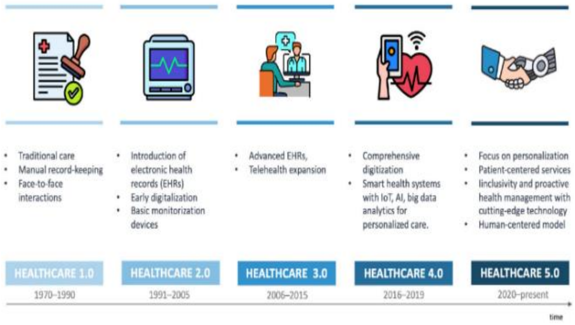
Traditional care
Manual record-keeping
Face-to-face interactions
Introduction of electronic health records (EHRs)
Early digitalization
Basic monitorization devices
Advanced EHRs,
Telehealth expansion
Comprehensive digitization
Smart health systems with IoT, AI, big data analytics for personalized care.
Focus on personalization
Patient-centered services
Iinclusivity and proactive health management with cutting-edge technology
Human-centered model
HEALTHCARE 1.0
1970–1990
HEALTHCARE 2.0
1991–2005
HEALTHCARE 3.0
2006–2015
HEALTHCARE 4.0
2016–2019
HEALTHCARE 5.0
2020–present
time

Fig. 4. Healthcare transition over time (Juliana Basulo-Ribeiro, 2024).

3.4. Healthcare 5.0 Security Protocol

• Authentication and key establishment protocols: Provide secure mutual authentication and key establishment among healthcare entities.

• Access control and key establishment protocols: Achieve secure access control among healthcare entities.

• Key distribution and management protocols: Secure key distribution and key management among healthcare entities.

• Intrusion detection protocols: Protect devices, servers, and users from malicious activities like remote hijacking, malware injection, DoS/DDoS, and suspicious flooding.

• Network-based intrusion detection systems and host-based intrusion detection systems are used to ensure system security.

4. Future Schemes of Healthcare 5.0

→ Unbreakable Security: Existing security frameworks are not fully secure or functional, making it challenging to develop solutions that can withstand multiple simultaneous attacks. Blockchain-related attacks, malware attacks, credentials guessing, and sensitive data leakage are possible attacks.

→ Effective Security Schemes: Smart healthcare devices in the healthcare 5.0 communication environment are resource-constrained, making it difficult to use resource-intensive complex algorithms. Low-cost security schemes are needed to protect these devices without sacrificing security.

→ Scalability Issues: Healthcare 5.0 is a large-scale heterogeneous network with different communication systems/devices and applications. Designing security frameworks for Healthcare 5.0 is challenging due to the diverse capabilities and needs of these systems.

→ Heterogeneity of Healthcare 5.0 Systems: Healthcare 5.0 uses a wide range of devices and communication protocols, making it difficult to design a security framework that supports and defends various devices and technology types.

→ Compatibility for Cross-Platform Existence: The heterogeneity of inbuilt networks poses a challenge in establishing a security framework for Healthcare 5.0. A robust and effective security framework is needed to ensure continuous connectivity across various healthcare platforms.

5. Conclusion

AI in Healthcare 5.0 revolutionizes the delivery and patient experience via a stunning confluence of cutting-edge technology and medical knowledge. Artificial Intelligence (AI), with its capacity to analyze intricate patterns, analyze large volumes of data, and make deft judgments, is set to historically significant improvements in patient care, diagnosis, and therapy. But even as we welcome these revolutionary possibilities, we must take care to maintain a balanced perspective that appreciates the combination of human intuition and AI's computing prowess. Achieving this balance will protect the fundamental principles of ethics, empathy, and compassion that form the basis of healthcare while also improving medical results. The success of AI in Healthcare 5.0 will be determined by its ability to enhance human capabilities and promote a healthier, more connected world.

References

Deepti Saraswat, P. B., A. Verma,Ravi Sharma. (2022). Explainable AI for Healthcare 5.0: Opportunities and Challenges. *IEEE access*, *10*, 84486–84517.

Elliot Mbunge, B. M., Sipho'esihle Jiyane, John Batani. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. *Global Health Journal*, *5*(4), 169-177.

Jaimon T Kelly, K. L. C., Enying Gong,Paul Scuffham. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *Journal of Medical Internet Research*, *22*(11).

Juliana Basulo-Ribeiro, L. T. (2024). The Future of Healthcare with Industry 5.0: Preliminary Interview-Based Qualitative Analysis. *MDPI Journal*, *16*(3).

Poonam Rani, P. K., Vibha Jain,Dr Sweety Nain. (2022). Blockchain-based IoT enabled health monitoring system. *The Journal of Supercomputing*, *78*(12).

Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Explainable AI for healthcare 5.0: opportunities and challenges. *Ieee Access*, *10*, 84486-84517.

Vivek Kaul, S. E., Seth A Gross. (2020). History of artificial intelligence in medicine. *National Library of Medicine*, *92*(4), 807-812.