JOURNAL OF ARTIFICIAL INTELLIGENCE AND ROBOTICS
Oct-Dec 2024, VOL. 1, ISSUE 4, pp. 35-40
https://doi.org/10.61577/jaiar.2025.1000021

RESEAPRO JOURNALS

Review

OPEN ACCESS

The role of IoT-Cloud in addressing the challenges in healthcare management

Om Prakash Mohapatra

Department of Computer Science and Engineering, Dayananda Sagar University, Bengaluru, India

ABSTRACT

Healthcare systems worldwide face significant challenges due to demographic shifts, notably the aging population, and the rising prevalence of chronic diseases. Traditional healthcare infrastructures struggle to meet these demands, prompting the need for innovative solutions. This review explores the potential of Internet of Things (IoT) and Cloud Computing technologies to revolutionize healthcare delivery, focusing on remote health monitoring and diagnostics. Wearable health monitoring systems, central to IoT-Cloud solutions, continuously collect and analyze health-related data, providing real-time insights into patient health. These systems offer significant benefits, including enhanced chronic disease management, improved elderly care, and increased healthcare access in remote areas. However, the deployment of IoT-Cloud solutions is not without challenges. Issues related to energy efficiency, data security, and interoperability must be addressed to ensure their effectiveness and sustainability. The review discusses strategies for improving sensor accuracy, energy management, and data security through advanced encryption techniques and robust authentication methods. Additionally, it highlights the importance of developing universal standards for device interoperability and the role of emerging technologies such as artificial intelligence and 5G in enhancing IoT-Cloud healthcare systems. The objective of this review is to provide a comprehensive overview of the current landscape, benefits, challenges, and future directions of IoT-Cloud healthcare solutions, emphasizing the need for continued research and innovation to realize their full potential in transforming healthcare delivery.

KEYWORDS

Internet of things (IoT); Cloud computing; Remote health monitoring; Chronic disease management; Data security

ARTICLE HISTORY

Received 20 November 2024; Revised 14 December 2024; Accepted 21 December 2024

Introduction

The global healthcare landscape is profoundly transformed, driven by demographic shifts and technological advancements. One of the most significant demographic trends is the aging population, characterized by increasing life expectancy and declining birth rates [1]. According to the United Nations, the global population aged 65 years or older is projected to increase from 703 million in 2019 to over 1.5 billion by 2050 [1]. This demographic shift poses substantial challenges to healthcare systems worldwide, as older adults often require more frequent and specialized medical care, particularly for managing chronic diseases such as diabetes, cardiovascular diseases, and neurodegenerative conditions [2]. Traditional healthcare systems are struggling to meet these growing demands. Resource limitations, including shortages of healthcare professionals and facilities, particularly in rural and underserved areas, exacerbate the situation. Additionally, the increasing prevalence of chronic conditions places a significant burden on healthcare infrastructures, as these diseases often require ongoing monitoring, treatment, and management [3]. This has led to a pressing need for innovative solutions that can enhance the efficiency, accessibility, and quality of healthcare services.

The advent of the Internet of Things (IoT) and Cloud Computing technologies offers a promising pathway to address these challenges. IoT refers to the interconnection of everyday objects, equipped with sensors and communication capabilities, to the internet, enabling data exchange and automation. IoT devices like wearable sensors and smart medical devices can continuously collect patient health-related data [4]. This data can include vital signs, physical activity, sleep patterns, and more, providing valuable insights into a patient's health status. When combined with Cloud Computing, IoT devices can transmit the collected data to cloud-based platforms, which can be stored, processed, and analyzed in real-time [5,6]. Cloud Computing offers scalable computing resources and sophisticated analytics tools, including machine learning and artificial intelligence algorithms, which can analyze vast amounts of health data to identify patterns, predict potential health issues, and provide personalized recommendations for treatment and lifestyle adjustments [7,8]. This integration, known as IoT-Cloud solutions, has the potential to revolutionize healthcare by enabling remote monitoring and diagnostics, thereby improving patient outcomes and reducing healthcare costs [9].

The benefits of IoT-Cloud healthcare solutions are particularly evident in the context of remote health monitoring and diagnostics. For patients living in rural or remote areas, access to healthcare facilities can be limited, making regular check-ups and monitoring challenging. IoT-Cloud systems can bridge this gap by allowing patients to be monitored from the comfort of their homes. For instance, wearable health monitoring systems can track vital signs and other health

***Correspondence:** Mr. Om Prakash Mohapatra, Department of Computer Science and Engineering, Dayananda Sagar University, Bengaluru, India, 562 112, e-mail: omprakashmohapatra007@gmail.com

metrics, alerting healthcare providers to any abnormalities that may require immediate attention. This not only improves access to care but also reduces the need for frequent hospital visits, which can be costly and time-consuming. Moreover, the real-time data provided by IoT devices can enable more proactive and preventative healthcare. By continuously monitoring health parameters, potential issues can be detected early, allowing for timely interventions before they escalate into more serious conditions. This shift from reactive to proactive healthcare is crucial in managing chronic diseases, where early detection and consistent management can significantly improve patient outcomes.

However, the implementation of IoT-Cloud solutions in healthcare is not without challenges. Concerns about data security and privacy are paramount, as sensitive health data is transmitted and stored digitally [10]. Ensuring the confidentiality and integrity of this data is critical to maintaining patient trust and compliance with regulatory standards. Additionally, issues related to the interoperability of devices and systems, data accuracy, and energy efficiency of wearable devices must be addressed to ensure the effective and sustainable deployment of these technologies. In summary, the integration of IoT and Cloud Computing in healthcare holds great promise for addressing the challenges posed by an aging population and the increasing burden of chronic diseases. By enabling remote monitoring and real-time data analysis, IoT-Cloud solutions can improve the accessibility, efficiency, and quality of healthcare services [11]. As the technology continues to evolve, it is essential to address the associated challenges to fully realize its potential in transforming healthcare delivery.

This expanded introduction provides a more comprehensive overview of the context, significance, and potential of IoT-Cloud solutions in healthcare.

Wearable health monitoring systems

Wearable health monitoring systems consist of several key components and technologies that enable the continuous collection and analysis of health-related data [12]. At the heart of these systems are wearable sensors that measure various physiological parameters. Common types include electrocardiogram (ECG) sensors, which track heart activity [13]; photoplethysmography (PPG) sensors, which measure blood oxygen levels [14]; and accelerometers, which monitor physical activity and detect falls [15]. Additional sensors, such as temperature sensors and galvanic skin response (GSR) sensors, can measure body temperature and assess stress levels, respectively [16]. These sensors transmit data using communication modules like Bluetooth, ZigBee, Wi-Fi, and Low-Power Wide-Area Networks (LPWAN) [17]. Bluetooth and Wi-Fi are ideal for short-range communication with high data rates, while LPWAN technologies, such as LoRa and NB-IoT [18], are suited for long-range, low-power applications, making them particularly useful for remote monitoring scenarios.

A Body Sensor Network (BSN) forms a crucial part of these systems. A BSN comprises multiple wearable sensors placed on or around the body, wirelessly communicating with a central processing unit like a smartphone or a specialized device [19]. This central unit serves as a data hub, collecting information from all connected sensors and sending it to cloud-based platforms for comprehensive analysis [19]. Initially, the data undergoes local pre-processing to filter out noise and perform basic analysis, minimizing the amount of data transmitted to the cloud. Once in the cloud, advanced analytics and machine learning algorithms can process the data to generate actionable insights [20].

The practical applications of wearable health monitoring systems are extensive, especially in the management of chronic diseases, elderly care, and remote patient monitoring in underserved regions. For individuals with chronic conditions such as diabetes or heart disease, these systems allow for continuous monitoring of vital signs, enabling early detection of potential issues and timely adjustments to treatment plans. In elderly care, these devices enhance safety by monitoring health metrics and detecting emergencies like falls, thus providing peace of mind to caregivers and families. Moreover, in rural or underserved areas where access to healthcare facilities may be limited, wearable health monitoring systems offer a critical solution for remote patient monitoring. This capability allows patients to receive consistent healthcare oversight without frequent hospital visits, which is particularly beneficial for managing chronic conditions and monitoring vulnerable populations.

The wearable health monitoring systems leverage advanced sensor technologies and communication networks to provide real-time, continuous health monitoring. They offer significant advantages in managing chronic diseases, supporting elderly care, and extending healthcare access to remote and underserved populations, thereby improving overall health outcomes. The data collected by these wearable sensors are transmitted via communication modules, such as Bluetooth, Wi-Fi, or low-power wide-area networks (LPWAN), to a central processing unit [17]. This unit can be a smartphone, tablet, or dedicated device, which serves as an intermediary between the sensors and cloud-based platforms. In the cloud, advanced data analytics, including machine learning algorithms, process and analyze the data, generating actionable insights for healthcare providers and patients [21].

Energy efficiency and sustainability

The long-term sustainability of wearable health monitoring systems heavily relies on their energy efficiency. These systems must function continuously and dependably, often requiring them to operate for extended periods without frequent recharging or battery replacement. Consequently, effective energy management is crucial. One approach involves using low-power microcontrollers and sensors, designed to consume minimal energy while maintaining high performance [22]. Additionally, the adoption of energy-efficient communication protocols, such as Bluetooth Low Energy (BLE) and ZigBee [23], further minimizes power consumption by reducing the energy required for data transmission between devices and processing units.

Beyond traditional power sources, energy harvesting techniques offer an innovative solution to extend the operational lifespan of wearable devices. These techniques involve capturing and converting ambient energy from the

https://doi.org/10.61577/jaiar.2025.1000021

surrounding environment into usable electrical power. For instance, solar energy harvesting utilizes photovoltaic cells to convert sunlight into electricity, while kinetic energy harvesting transforms mechanical energy from body movements into electrical energy [24]. Thermal energy harvesting captures heat from the body or the environment, converting temperature differences into electrical power [25]. These methods not only prolong battery life but also reduce reliance on conventional batteries, thereby minimizing electronic waste [26]. However, energy harvesting poses challenges, including the variability of ambient energy sources and the need for efficient energy conversion technologies [27].

Sustainability in wearable health monitoring systems also extends to the materials and design of the devices. The use of biodegradable and recyclable materials in the manufacturing process is essential to reduce the environmental footprint of these devices [28]. Materials such as biodegradable polymers can decompose naturally, minimizing the impact of discarded devices on the environment [28]. Additionally, the recyclability of components allows for the recovery and reuse of valuable materials, further promoting environmental sustainability [29]. The design of wearable devices must also prioritize user comfort and biocompatibility, ensuring that the materials used do not cause irritation or allergic reactions, especially for devices worn for prolonged periods [30,31]. Ergonomic design and the use of soft, flexible materials enhance comfort, encouraging consistent use and improving the overall effectiveness of health monitoring [32].

In summary, the sustainability and energy efficiency of wearable health monitoring systems are critical considerations in their development and deployment [33]. By integrating low-power technologies, utilizing energy harvesting techniques, and employing sustainable materials, these systems can operate efficiently over extended periods, reduce their environmental impact, and provide reliable health monitoring for users [34]. As the demand for wearable technology grows, ongoing research and innovation in these areas will be key to advancing the field and ensuring that these devices are both effective and environmentally responsible.

Data security and privacy

The shift towards digital healthcare systems has significantly enhanced the capabilities and convenience of health monitoring, but it has also introduced critical concerns regarding data security and privacy. As wearable devices and Internet of Things (IoT) systems collect and transmit sensitive personal health information, safeguarding this data against unauthorized access and breaches is essential [35]. To address these concerns, a multi-faceted approach to data security is necessary, involving encryption techniques, robust authentication methods, and adherence to regulatory frameworks [36].

Data encryption and security protocols

Data encryption is a fundamental component of securing health information. Techniques such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption are commonly used to protect data during transmission and storage [37]. AES is a symmetric encryption algorithm that ensures data confidentiality by transforming plaintext into ciphertext using a secret key [38]. It is widely used due to its efficiency and strong security. RSA, on the other hand, is an asymmetric encryption algorithm that uses a pair of keys—one public and one private—to encrypt and decrypt data [39]. This method is particularly useful for secure key exchange and digital signatures. Both AES and RSA contribute to secure data transmission by encrypting health information as it moves between wearable devices, communication modules, and cloud servers, thereby preventing unauthorized access [40].

In addition to encryption, secure data storage is vital for maintaining data integrity and confidentiality [41]. This involves using secure servers with encrypted databases and implementing access controls to restrict data retrieval to authorized personnel only [42]. Data should be encrypted both at rest and in transit to ensure comprehensive protection against potential breaches [43].

Authentication and access control

Effective authentication and access control mechanisms are crucial for ensuring that only authorized individuals can access sensitive health data [44]. Multi-factor authentication (MFA) enhances security by requiring users to provide two or more verification factors before granting access [45]. These factors typically include something the user knows (a password), something the user has (a security token), and something the user is (biometric data) [46]. MFA adds an extra layer of protection, making it significantly more difficult for unauthorized users to gain access to sensitive information [47]. Biometric verification is another advanced authentication method that leverages unique biological characteristics, such as fingerprints, facial recognition, or iris patterns, to authenticate users [48]. This method is particularly effective in providing a high level of security while maintaining user convenience. The integration of biometric verification in wearable devices ensures that only the registered user can access their personal health data, further safeguarding privacy.

Regulatory and Compliance Considerations

Regulatory frameworks play a crucial role in protecting patient privacy and ensuring data security. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) sets standards for safeguarding protected health information (PHI) [49]. HIPAA mandates that healthcare providers, insurers, and their business associates implement security measures to protect patient data and provides patients with rights to access, amend, and control their health information [50,51].

Similarly, the General Data Protection Regulation (GDPR) in the European Union establishes comprehensive data protection standards for personal data, including health information. GDPR emphasizes the need for explicit consent from individuals for data collection and processing, and it grants individuals the right to access, correct, and delete their data [52]. Both HIPAA and GDPR enforce strict compliance requirements and impose penalties for non-compliance, thus ensuring that healthcare organizations uphold the highest standards of data security and privacy [53].

In summary, securing healthcare data in the digital age requires a multi-layered approach encompassing robust

https://doi.org/10.61577/jaiar.2025.1000021

encryption methods, advanced authentication techniques, and adherence to stringent regulatory standards. By implementing these measures, wearable health monitoring systems can effectively protect sensitive personal health information and maintain patient trust in the digital healthcare ecosystem.

Challenges and Future Directions

Despite the substantial advancements in IoT-Cloud healthcare solutions, several challenges must be addressed to fully realize their potential. One significant challenge lies in sensor accuracy and signal quality. Wearable sensors can be affected by motion artifacts, environmental conditions, and improper sensor placement, leading to variability in data quality [54]. Research is ongoing to improve sensor precision and develop algorithms that can effectively filter out noise and artifacts [55]. Techniques such as advanced signal processing and calibration methods are crucial for enhancing sensor reliability and ensuring accurate health monitoring.

Another pressing challenge is achieving interoperability and standardization among diverse devices and systems. The current lack of universal standards in sensor technologies and communication protocols can hinder the seamless integration of various components within an IoT-Cloud ecosystem [56,57]. To address this, efforts are being made to develop comprehensive standards and frameworks that facilitate the integration and exchange of data across different platforms and devices. Establishing these standards is vital for creating a cohesive system where devices from various manufacturers can work together seamlessly, improving the overall functionality and user experience [57].

Scalability and data management present additional concerns, particularly as the number of connected devices and users continues to grow. Wearable devices generate vast amounts of data, which must be efficiently managed and processed [12]. Cloud platforms need to be capable of dynamically scaling resources to handle increasing data loads without sacrificing performance or security [57]. Advances in cloud computing, such as the adoption of distributed architectures and enhanced data storage solutions, are essential for addressing these scalability issues and ensuring that data processing remains efficient and secure.

Emerging technologies and innovations also play a crucial role in addressing these challenges. Integrating artificial intelligence (AI) and machine learning in data analysis can significantly enhance the ability to interpret complex health data, identify patterns, and provide actionable insights [10]. Furthermore, the deployment of 5G networks and edge computing technologies promises to improve data transmission speeds and reduce latency, enabling more effective real-time monitoring and analysis [58]. These advancements are expected to drive further innovation in IoT-Cloud healthcare solutions, making them more efficient and responsive.

In conclusion, while IoT-Cloud healthcare solutions offer significant benefits, including enhanced health monitoring and improved patient care, several challenges must be overcome. Addressing issues related to sensor accuracy, interoperability, scalability, and data management is crucial for maximizing the potential of these technologies. The ongoing development of universal standards, advancements in AI and machine learning, and the integration of 5G and edge computing will play key roles in overcoming these challenges. Continued research and innovation are essential to advancing IoT-Cloud solutions, ensuring they are both sustainable and secure, and ultimately transforming the future of healthcare.

Conclusions

IoT-Cloud solutions for remote health monitoring are set to revolutionize healthcare by integrating wearable sensors, cloud computing, and real-time data analytics. These systems enable continuous monitoring, enhance the management of chronic conditions, support elderly care, and expand access to quality healthcare, particularly in rural and underserved areas. The benefits include improved health outcomes through timely interventions and reduced healthcare costs by minimizing hospital visits. However, challenges like energy efficiency, data security, and interoperability must be addressed for widespread adoption. Low-power technologies and energy harvesting are key to sustaining wearable devices. Robust encryption and compliance with frameworks like HIPAA and GDPR are essential for safeguarding patient data and maintaining trust. Universal device and system interoperability standards are critical to seamless integration and data exchange.

Sustainability and security are paramount as remote monitoring grows. Using biodegradable materials and energy-efficient designs reduces environmental impact, while stringent security measures protect sensitive health data. Future research should focus on improving sensor accuracy, advancing universal standards, and enhancing data management. Innovations in AI, machine learning, 5G, and edge computing will further boost the capabilities of IoT-Cloud healthcare systems. In summary, continued advancements in technology, sustainability, and security will drive the success of IoT-Cloud healthcare, revolutionizing patient care while contributing to a more sustainable future.

Disclosure Statement

No potential conflict of interest was reported by the author.

References

1. Laskar BI. Population ageing: Gender and health issues. In the plural social sphere. Routledge India. 2024:148-167.
2. Osareme J, Muonde M, Maduka CP, Olorunsogo TO, Omotayo O. Demographic shifts and healthcare: A review of aging populations and systemic challenges. Int J Sci Res. 2024;11(1):383-395. https://doi.org/10.30574/ijsra.2024.11.1.0067
3. World Health Organization. Noncommunicable Disease, Mental Health Cluster. Innovative care for chronic conditions: building blocks for action: global report. World Health Organization; 2002.
4. Wan J, AAH Al-awlaqi M, Li M, O'Grady M, Gu X, Wang J, Cao N. Wearable IoT enabled real-time health monitoring system. EURASIP J Wirel Commun Netw. 2018(1):1-0. https://doi.org/10.1186/s13638-018-1308-x
5. Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. Future generation computer systems. 2016;56:684-700. https://doi.org/10.1016/j.future.2015.09.021
6. Rao BP, Saluia P, Sharma N, Mittal A, Sharma SV. Cloud computing for Internet of Things & sensing based applications. In2012 sixth international conference on sensing technology (ICST).IEEE. 2012; 374-380. https://doi.org/10.1109/ICSensT.2012.6461705

https://doi.org/10.61577/jaiar.2025.1000021

7. Butt UA, Mehmood M, Shah SB, Amin R, Shaukat MW, Raza SM, et al. A review of machine learning algorithms for cloud computing security. Electronics. 2020;26;9(9):1379. https://doi.org/10.3390/electronics9091379
8. Pronk NP, Anderson LH, Crain AL, Martinson BC, O'Connor PJ, Sherwood NE, et al. Meeting recommendations for multiple healthy lifestyle factors: prevalence, clustering, and predictors among adolescent, adult, and senior health plan members. Am J Prev Med. 2004;27(2):25-33. https://doi.org/10.1016/j.amepre.2004.04.022
9. Akhbarifar S, Javadi HH, Rahmani AM, Hosseinzadeh M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Pers Ubiquitous Comput. 2023; 27(3):697-713. https://doi.org/10.1007/s00779-020-01475-3
10. Adeniyi AO, Arowoogun JO, Okolo CA, Chidi R, Babawarun O. Ethical considerations in healthcare IT: A review of data privacy and patient consent issues. World J Adv Res Rev. 2024;21(2): 1660-1668. https://doi.org/10.30574/wjarr.2024.21.2.0593
11. Mahmud R, Koch FL, Buyya R. Cloud-fog interoperability in IoT-enabled healthcare solutions. InProceedings of the 19th international conference on distributed computing and networking 2018;4:1-10. https://doi.org/10.1145/3154273.3154347
12. Anikwe CV, Nweke HF, Ikegwu AC, Egwuonwu CA, Onu FU, Alo UR, et al. Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect. Expert Syst Appl. 2022;202:117362. https://doi.org/10.1016/j.eswa.2022.117362
13. Ramasamy S, Balan A. Wearable sensors for ECG measurement: a review. Sens Rev. 2018;38(4):412-419. https://doi.org/10.1108/SR-06-2017-0110
14. Ma G, Zhu W, Zhong J, Tong T, Zhang J, Wang L. Wearable ear blood oxygen saturation and pulse measurement system based on PPG. In2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ ATC/CBDCom/IOP/SCI) 2018;111-116. IEEE. https://doi.org/10.1109/SmartWorld.2018.00054
15. Lee RY, Carlisle AJ. Detection of falls using accelerometers and mobile phone technology. Age and ageing. 2011;40(6):690-696. https://doi.org/10.1093/ageing/afr050
16. Basjaruddin NC, Syahbarudin F, Sutjiredjeki E. Measurement device for stress level and vital sign based on sensor fusion. Healthcare informatics research. 2021;27(1):11-28. https://doi.org/10.4258/hir.2021.27.1.11
17. Onumanyi AJ, Abu-Mahfouz AM, Hancke GP. Low power wide area network, cognitive radio and the Internet of Things: Potentials for integration. Sensors. 2020;20(23):6837. https://doi.org/10.3390/s20236837
18. Malik PK, Bilandi N, Gupta A. Narrow band-IoT and long-range technology of IoT smart communication: Designs and challenges. Comput Indus Eng. 2022;172:108572. https://doi.org/10.1016/j.cie.2022.108572
19. Gravina R, Fortino G. Wearable body sensor networks: state-of-the-art and research directions. IEEE Sens J. 2020;21(11): 12511-12522. https://doi.org/10.1109/JSEN.2020.3044447
20. Sharma N, Shamkuwar M. Big data analysis in cloud and machine learning. Big data processing using spark in cloud. 2019:51-85. https://doi.org/10.1007/978-981-13-0550-4_3
21. Bayyapu S, Turpu RR, Vangala RR. Advancing healthcare decisionmaking: The fusion of machinelearning, predictive analytics, andcloud technology. International Journal of Computer Engineering and Technology (IJCET). 2019;10(5):157-170.
22. Ekanayake V, Kelly IV C, Manohar R. An ultra low-power processor for sensor networks. InProceedings of the 11th international conference on Architectural support for programming languages and operating systems. 2004;27-36. https://doi.org/10.1145/1024393.1024397
23. Gomez C, Oller J, Paradells J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. sensors. 2012;12(9):11734-11753. https://doi.org/10.3390/s120911734
24. Kang X, Jia S, Lin Z, Zhang H, Wang L, Zhou X. Flexible wearable hybrid nanogenerator to harvest solar energy and human kinetic energy. Nano Energy. 2022;103:107808. https://doi.org/10.1016/j.nanoen.2022.107808
25. Thielen M, Sigrist L, Magno M, Hierold C, Benini L. Human body heat for powering wearable devices: From thermal energy to application. Energy Conv Manag. 2017;131:44-54. https://doi.org/10.1016/j.enconman.2016.11.005
26. Roy JJ, Rarotra S, Krikstolaityte V, Zhuoran KW, Cindy YD, Tan XY, et al. Green recycling methods to treat lithium-ion batteries E-waste: a circular approach to sustainability. Advanced Materials. 2022;34(25):2103346. https://doi.org/10.1002/adma.202103346
27. Ku ML, Li W, Chen Y, Liu KR. Advances in energy harvesting communications: Past, present, and future challenges. IEEE Communications Surveys & Tutorials. 2015;18(2):1384-1412. https://doi.org/10.1109/COMST.2015.2497324
28. Cenci MP, Scarazzato T, Munchen DD, Dartora PC, Veit HM, Bernardes AM, et al. Eco-friendly electronics—a comprehensive review. Adv Mater Technol. 2022;7(2):2001263. https://doi.org/10.1002/admt.202001263
29. Haider TP, Völker C, Kramm J, Landfester K, Wurm FR. Plastics of the future? The impact of biodegradable polymers on the environment and on society. Angew Chem Int Ed. 2019;58(1): 50-62. https://doi.org/10.1002/anie.201805766
30. Ribeiro MC, Fiúza A, Ferreira A, Dinis MD, Meira Castro AC, Meixedo JP, et al. Recycling approach towards sustainability advance of composite materials' industry. Recycling. 2016;1(1):178-93. https://doi.org/10.3390/recycling1010178
31. Jian S. Industrial design of wearable intelligent devices based on wireless networks. Measurement: Sensors. 2023;30:100934. https://doi.org/10.1016/j.measen.2023.100934
32. Chander H, Burch RF, Talegaonkar P, Saucier D, Luczak T, Ball JE, et al. Wearable stretch sensors for human movement monitoring and fall detection in ergonomics. Int J Environ Res Public Health. 2020;17(10):3554. https://doi.org/10.3390/ijerph17103554
33. Nia AM, Mozaffari-Kermani M, Sur-Kolay S, Raghunathan A, Jha NK. Energy-efficient long-term continuous personal health monitoring. IEEE Trans. Multi-Scale Comput. Syst. 2015;1(2):85-98. https://doi.org/10.1109/TMSCS.2015.2494021
34. Ali A, Shaukat H, Bibi S, Altabey WA, Noori M, Kouritem SA. Recent progress in energy harvesting systems for wearable technology. Energy Strategy Reviews. 2023;49:101124. https://doi.org/10.1016/j.esr.2023.101124
35. Maras MH. Internet of Things: security and privacy implications. Int'l Data Priv. L. 2015;5:99. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/intldatpc5&div=15&id=&page=
36. Odeh A, Taleb AA. A multi-faceted encryption strategy for securing patient information in medical imaging. Mobile network ubiquitous computing and dependable application (JoWUA). 2023;14(4):164-176. https://doi.org/10.58346/JOWUA.2023.I4.012
37. Alsaffar DM, Almutiri AS, Alqahtani B, Alamri RM, Alqahtani HF, Alqahtani NN, et al. Image encryption based on AES and RSA algorithms. In2020 3rd International Conference on Computer Applications & Information Security (ICCAIS). IEEE. 2020;1-5. https://doi.org/10.1109/ICCAIS48893.2020.9096809
38. Lu Z, Mohamed H. A complex encryption system design implemented by AES. J Inf Secur. 2021;12(2):177-187. https://doi.org/10.4236/jis.2021.122009
39. Jamgekar RS, Joshi GS. File encryption and decryption using secure RSA. Int J Emerg Sci Eng (IJESE). 2013;1(4):11-24.
40. Popoola O, Rodrigues MA, Marchang J, Shenfield A, Ikpehai A, Popoola J. An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security.

https://doi.org/10.61577/jaiar.2025.1000021

Internet of Things. 2024;27:101314. https://doi.org/10.1016/j.iot.2024.101314
41. Aldossary S, Allen W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. Int J Adv Comput Sci Appl. 2016;7(4). http://dx.doi.org/10.14569/IJACSA.2016.070464
42. Zhou L, Varadharajan V, Hitchens M. Achieving secure role-based access control on encrypted data in cloud storage. IEEE Trans Inf Forensics Secur. 2013;8(12):1947-1960. https://doi.org/10.1109/TIFS.2013.2286456
43. Ulybyshev D. Data Protection in Transit and at Rest with Leakage Detection (Doctoral dissertation, Purdue University).
44. Li M, Yu S, Ren K, Lou W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. InSecurity and Privacy in Communication Networks: 6th Iternational ICST Conference, SecureComm 2010, Singapore, 7-9, 2010. Proceedings 6 2010;89-106. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16161-2_6
45. Das S, Wang B, Kim A, Camp LJ. MFA is a necessary chore!: Exploring user mental models of multi-factor authentication technologies. InHICSS 2020;:1-10. http://dx.doi.org/10.24251/HICSS.2020.669
46. O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE. 2003;91(12):2021- 2040.
47. Hussain MI, He J, Zhu N, Sabah F, Zardari ZA, Hussain S, et al. AAAA: SSO and MFA implementation in multi-cloud to mitigate rising threats and concerns related to user metadata. Applied Sciences. 2021;11(7):3012. https://doi.org/10.3390/app11073012
48. Jain AK, Deb D, Engelsma JJ. Biometrics: Trust, but verify. IEEE Trans Biom Behav Identity Sci. 2021;4(3):303-323. https://doi.org/10.1109/TBIOM.2021.3115465
49. Shoaf HR. Health insurance portability and accountability act (HIPAA): Protected health information (PHI)-Physician's Office Challenges. Plastic and Aesthetic Nursing. 2003;23(2):75-77.
50. Huddleston A, Hedges R. Liability for health care providers under HIPAA and state privacy laws. Seton Hall L Rev. 2020;51:1585.
51. Hoffman S. Privacy and security. Protecting patients' health information. N Engl J Med. 2022;387(21). https://doi.org/10.1056/NEJMp2201676
52. Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. J Cybersecur. 2018;4(1):tyy001. https://doi.org/10.1093/cybsec/tyy001
53. Gupta R. Navigating regulatory landscapes in healthcare IT: Upholding HIPAA and GDPR compliance. Adv Comput Sci. 2020;3(1):1-5.
54. Böttcher S, Vieluf S, Bruno E, Joseph B, Epitashvili N, Biondi A, et al. Data quality evaluation in wearable monitoring. Scientific reports. 2022;12(1):21412. https://doi.org/10.1038/s41598-022-25949-x
55. Han S, Meng Z, Omisore O, Akinyemi T, Yan Y. Random error reduction algorithms for MEMS inertial sensor accuracy improvement-a review. Micromachines. 2020;11(11):1021. https://doi.org/10.3390/mi11111021
56. Vermesan O, Friess P, editors. Internet of things: converging technologies for smart environments and integrated ecosystems. River publishers. 2013.
57. Hwang K, Bai X, Shi Y, Li M, Chen WG, Wu Y. Cloud performance modeling with benchmark evaluation of elastic scaling strategies. IEEE Trans Parallel Distrib. Syst. 2015;27(1):130-143. https://doi.org/10.1109/TPDS.2015.2398438
58. Hassan N, Yau KL, Wu C. Edge computing in 5G: A review. IEEE Access. 2019;7:127276-127289. https://doi.org/10.1109/ACCESS.2019.2938534

https://doi.org/10.61577/jaiar.2025.1000021