National Research Journal of Information Technology & Information Science
Volume No: 11, Issue No: 2, Year: 2024 (July-December)
PP: 44-51
ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

IoT IN HEALTHCARE: A REVIEW OF CLOUD-INTEGRATED ARCHITECTURES, EFFICIENCY, AND SECURITY ISSUES

Gurwinder Singh

Department of Computer Science and Applications, Sikh National College, Banga, India

ABSTRACT

Recent studies have increasingly focused on the role of Internet of Things (IoT) technologies in transforming healthcare systems. With rapid growth in applications such as remote health monitoring and fitness tracking, IoT has become a key enabler in improving patient care and system efficiency. A significant body of research has explored ways to enhance monitoring accuracy and overall performance in IoT-driven healthcare solutions.

This work examines various architectural approaches used in IoT healthcare, with particular attention to cloud-integrated systems that support scalable data storage and processing. Critical factors such as accuracy and energy efficiency remain central challenges, and many studies aim to optimize these aspects to ensure reliable and sustainable operation. Additionally, data management strategies within cloud-supported IoT frameworks are analyzed to understand how large volumes of health data can be handled effectively.

The review also highlights the strengths and weaknesses of existing IoT-based healthcare systems. Many solutions demonstrate strong capabilities in detecting symptoms early and supporting disease prediction with high precision. Notably, IoT applications designed for elderly care provide practical and efficient tools for continuous health monitoring. However, several challenges persist, including high energy consumption, limited resource availability, and security concerns arising from the use of multiple interconnected devices.

1.INTRODUCTION

The Internet of Things (IoT) has rapidly become an integral part of modern life, finding applications across a wide range of domains. Its growing significance is especially evident in healthcare, where IoT-based systems are being developed to support efficient patient monitoring and timely emergency response[1,2]. These technologies are also widely used in e-health applications, enabling early identification of medical conditions, real-time alerts during critical situations, and support for computer-assisted rehabilitation.

In today's digital era, smartphones play a crucial role in daily life and are increasingly integrated with various sensors to track and monitor individual health conditions. Such sensor-based monitoring systems collect data from hospital wards and diagnostic devices, which can then be analyzed to enable automated and more effective healthcare management. IoT-driven healthcare solutions also contribute to better tracking and monitoring of patients, leading to improved utilization and management of healthcare resources[3,4].

Furthermore, cloud computing plays a vital role in supporting these systems by managing large volumes of healthcare data. It offers advantages such as flexible resource sharing, seamless integration of data services, scalable storage, and the ability to process data in parallel. At the same time, it helps address security concerns by enabling early detection and management of potential threats[5].

In IoT-based healthcare systems, wearable devices and implanted sensors typically operate with limited battery capacity. Frequent charging of these devices, along with associated mobile units, can become inconvenient for patients and may also require assistance from

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

healthcare staff, ultimately affecting the overall user experience[6]. In addition, cloud data centers that support these systems consume significant amounts of energy, leading to higher operational costs. Despite this, healthcare monitoring solutions demand cloud services that can deliver low latency while maintaining energy efficiency[7].

Security is another critical concern in healthcare monitoring, as sensitive patient data is vulnerable to tampering or unauthorized access by attackers. This makes it essential to design IoT-based healthcare systems that prioritize privacy and ensure secure data transmission between devices and healthcare providers. Although some studies have attempted to strengthen data security in IoT environments, challenges still remain[8-10].

In this context, existing research on IoT healthcare systems is often evaluated based on factors such as accuracy, computational efficiency, and the challenges faced during implementation. One important application area is the monitoring of cardiac patients using sensor-based technologies. For instance, electrocardiogram (ECG) data collected through sensors can be transmitted to medical professionals, enabling timely analysis and better decision-making in patient care.

2. LITERATURE REVIEW

The Internet of Things (IoT) is rapidly evolving as a key technology within the modern internet ecosystem, enabling real-time interaction between connected devices. Its widespread adoption across various sectors is driven by the transformation of ordinary objects into intelligent, connected systems. In healthcare, this advancement has had a significant impact on patient monitoring, administrative processes, and clinical services by enabling continuous tracking of physiological data.

In typical IoT-based healthcare setups, patients are equipped with sensors that collect health-related information. This data is linked to control systems and transmitted to monitoring units for analysis. In many cases, the collected data is stored in cloud platforms, which offer scalable storage and help manage large volumes of information securely. However, security remains a major concern, as transmitting sensitive data from sensors to cloud servers can expose it to risks such as loss of confidentiality and data integrity. Ensuring secure communication is particularly challenging due to the limited computational capabilities of many IoT devices, which restrict the use of complex encryption techniques.

Cloud computing plays an important role in addressing data storage and accessibility needs, as its distributed nature allows healthcare data to be accessed remotely by both patients and medical professionals. The integration of IoT and cloud technologies enables real-time data processing, but it also introduces architectural complexity in managing data exchange between devices and cloud systems. To address this issue, researchers have proposed innovative frameworks designed to simplify IoT-cloud integration and efficiently handle both real-time and non-real-time data[11].

One such approach is a Service Management Framework for IoT devices in the cloud (SMFIC), which is structured into three layers and includes key functional components. The first layer, known as the consumer layer, gathers data from sources such as smart homes, patients, social platforms, and healthcare services. The second layer, the service provider layer, is responsible for resource sharing, virtualization, service management, and ensuring security and privacy. The final layer, the middle layer, acts as an intermediary, coordinating services between providers and consumers based on the availability of resources.

Kumar and Gandhi [12] introduced an IoT-based framework that integrates machine learning techniques for the early detection of heart diseases. Their approach is built on a three-layer

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

architecture, where data is first collected from wearable sensors, then stored in a cloud environment, and finally analyzed using a regression-based prediction model. For implementation, they utilized Apache HBase for cloud data storage and Apache Mahout for performing predictive analytics. The results of their study demonstrate that this system can effectively support early diagnosis of heart-related conditions, enabling timely medical intervention.

Parthasarathy and Vivekanandan [13] developed an IoT-based system aimed at monitoring patients with arthritis and enabling early diagnosis of the condition. Their framework is structured into three stages. In the first stage, data is collected from various sensors attached to the patient. The second stage involves storing this data in a cloud environment. In the final stage, the collected information—such as indicators like swelling and uric acid (UA) levels—is analyzed and optimized to support diagnosis. The system was implemented using technologies such as Apache Redshift for data management and OpenStack for cloud infrastructure.

Kim and Chung [14] proposed a system in which sensor devices were strategically placed within a typical home environment, such as living rooms and other frequently used spaces, to monitor patients with chronic illnesses during their daily routines. However, the approach did not support real-time data processing, which limited its responsiveness. Additionally, the overall implementation was relatively expensive. To improve cost efficiency, the study suggests that replacing camera-based monitoring with sensor-based solutions could significantly reduce expenses while still maintaining effective patient monitoring.

In study [15], a Temporal Fuzzy Ant Miner Tree (TFAMT) classifier was introduced, combining concepts from Ant Colony Optimization (ACO), decision trees, and fuzzy logic rules to classify medical data more effectively. This approach is particularly useful for supporting elderly individuals by identifying age-related health conditions and managing their medication requirements. Within an IoT-based environment, real-time data is gathered through advanced sensors, and health issues are detected by analyzing both physical activities and behavioral patterns in a home setting.

Several studies have explored the use of IoT technologies to support elderly individuals by enabling continuous monitoring of their health and daily activities [16–18]. In many cases, these monitoring services are integrated into broader social or assistive platforms, making it easier to track the well-being of older adults. One of the most critical concerns for the elderly is the risk of falls, which, if not addressed promptly, can lead to serious or even fatal consequences.

To tackle this issue, researchers have developed fall detection algorithms that can identify when an individual has fallen within a predefined area. These systems often rely on technologies such as RFID and location-tracking data to accurately determine the position of the person. By analyzing this information, the system can quickly detect incidents and pinpoint where the fall occurred.

Such IoT-based solutions allow elderly individuals to continue living independently in their own homes while ensuring their safety. At the same time, they enable real-time health monitoring and can automatically send alerts to hospitals or family members in case of emergencies, providing timely assistance when needed.

3. INTEGRATION OF IoT WITH CLOUD

In mobile application–based remote healthcare systems, data collected from IoT devices is typically stored and processed using cloud platforms. Cloud computing provides key

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

advantages such as flexibility, scalability, and access to powerful resources for handling large volumes of data. Since health-related information is gathered from multiple sensors, it is efficiently organized and stored in centralized cloud repositories. Many researchers have leveraged cloud integration to streamline medical processes and enhance overall healthcare delivery.

For instance, physiological data collected from individuals can be stored in various formats within cloud storage systems. Once the user-side subsystem gathers data from IoT-enabled medical devices, it is transmitted to the cloud for further analysis and diagnosis. In case of any abnormal condition, alerts are automatically sent to doctors, hospitals, or caregivers to ensure timely intervention as shown in figure 1.

To improve system performance, researchers have also proposed advanced architectures such as the Hierarchical Computing Architecture (HiCH), which enables autonomous data processing at the edge layer, reducing the burden on centralized systems. Network latency remains a significant challenge in remote healthcare monitoring[16]. To address this, frameworks like UbeHealth have been introduced to analyze network delays and optimize Quality of Service (QoS), particularly in smart city environments, thereby enhancing system responsiveness[17].

Additionally, intelligent diagnostic approaches, such as fuzzy rule-based neural classifiers, have been developed to support disease prediction and minimize health risks. These methods rely on secure cloud-based data processing mechanisms that include stages like data retrieval, aggregation, partitioning, and merging, ensuring efficient and reliable analysis of healthcare data[18].

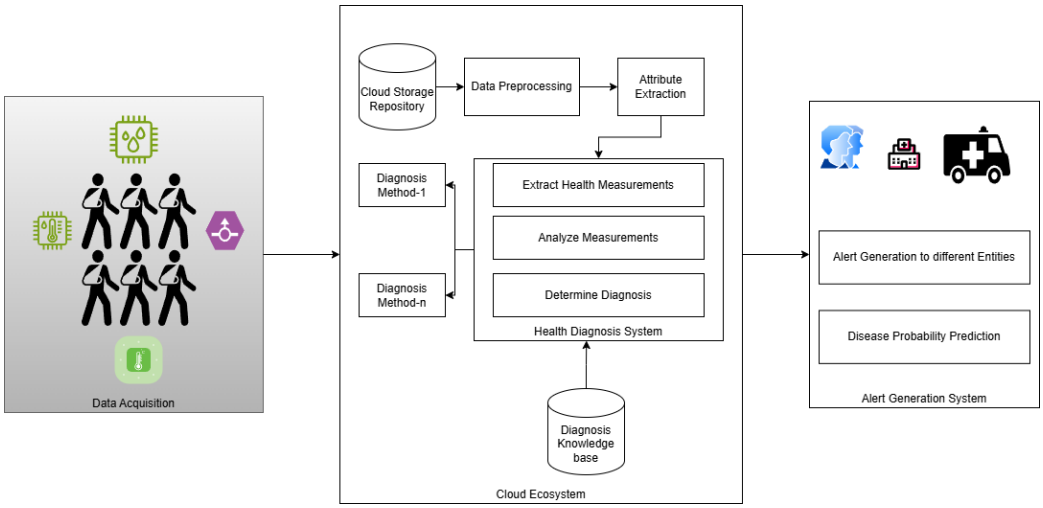

Figure 1: Cloud integration with Healthcare IoT system

4. IoT SECURITY

Security remains one of the most critical challenges in IoT-based healthcare systems, as sensor data can be vulnerable to unauthorized access by attackers. This makes it essential to evaluate and strengthen modern security mechanisms within IoT environments. To address these concerns, a privacy-aware data placement approach, known as IDP, has been proposed [19]. This method focuses on reducing data access time, improving resource utilization, and lowering energy consumption while maintaining strict privacy constraints. It employs the Non-dominated Sorting Genetic Algorithm II (NSGA-II) to achieve a balance between privacy protection and energy efficiency.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

In another approach, sensitive health data is processed locally on user devices to ensure trust and privacy, while recommendation services are handled through cloud-based healthcare platforms [20]. Security enhancements have also been explored using encryption techniques such as radio-frequency identification (RFID), which help protect medical data during transmission in IoT systems [21].

Given the critical nature of health data flow across networks, researchers have proposed frameworks that combine biometric authentication with lightweight security mechanisms suitable for resource-constrained wearable devices [29]. Additionally, in the context of the Internet of Medical Things (IoMT), advanced cryptographic methods have been introduced to strengthen data protection. For example, cloud-based healthcare systems may include multiple components such as an Authentication Server (AS), a Key Generation Center (KGC), and a Database Server (DS) to manage secure communication.

A lattice-based secure cryptographic scheme has also been proposed to safeguard healthcare data. This approach typically involves multiple stages, including system initialization, key generation, data encryption, and decryption. In this process, mathematical structures such as lattice-based polynomial vectors are used to generate public and private keys, which are securely shared between system components. When a user requests access to medical data, secure key exchange mechanisms ensure that only authorized entities can decrypt and process the information. Compared to existing methods, this approach demonstrates improvements in both communication efficiency and computational cost, making it suitable for secure IoT healthcare applications.

4. IoT HEALTHCARE CHALLENGES

The Internet of Things (IoT) is widely used across various domains and plays a significant role in enhancing healthcare services, including patient monitoring and smart home solutions for individuals with chronic conditions such as diabetes. While these advancements offer many benefits, several challenges still affect the efficiency and reliability of IoT-based healthcare systems.

a. One of the major advantages of IoT is the flexibility it provides, allowing patients to receive continuous care while staying in their homes instead of being confined to hospitals. However, some wearable devices and sensors can cause discomfort, which may affect user acceptance and long-term usage.

b. Data transmission is another critical concern. Health data collected from sensors is sent through multiple stages—from the sensing device to control units and then to monitoring centers. During this process, noise and interference can degrade data quality. Designing robust system architectures and applying effective noise reduction techniques are essential to preserve data accuracy.

c. In many existing systems, particularly those involving ECG monitoring, data analysis is often performed using supervised methods. While effective, these approaches can be costly and sometimes prone to errors. Incorporating machine learning techniques can improve accuracy, enhance efficiency, and reduce operational costs.

d. Energy consumption is also a significant issue, as the growing number of connected sensors and devices increases power requirements and leads to higher energy usage. Optimization algorithms can help manage and reduce energy consumption in such systems.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

e. Additionally, handling large volumes of data from multiple users requires substantial storage and computational resources. Cloud computing offers a practical solution for data storage and processing, although integrating IoT with cloud systems introduces added complexity.

f. Finally, privacy and security remain major concerns. IoT devices are often vulnerable to cyberattacks, and their limited computational capabilities make it challenging to implement strong encryption techniques. Ensuring secure data transmission and protecting user privacy are therefore critical areas that require ongoing research and development.

5. CONCLUSION

IoT technology enables effective remote monitoring of patients, making it especially valuable for providing timely emergency support, particularly for individuals with heart conditions. The primary aim of this review is to examine the different research efforts focused on IoT-based healthcare systems. Many existing studies demonstrate strong capabilities in continuously monitoring patients and transmitting health data to centralized monitoring units.

A significant portion of this research focuses on ECG-based monitoring systems, where machine learning techniques are used to analyze signals and predict potential health issues at an early stage. Some studies also address energy efficiency by applying optimization algorithms to reduce power consumption, highlighting the importance of designing systems that operate with minimal energy while maintaining high performance.

Despite these advancements, privacy remains a key concern in IoT healthcare due to the limited computational and storage capabilities of devices, which restrict the use of advanced encryption techniques. Cloud computing plays an important role in managing large volumes of healthcare data, although integrating IoT with cloud systems can increase system complexity.

Overall, current IoT-based healthcare solutions offer reliable and scalable patient monitoring, including support for elderly care through the use of sensors, cameras, and communication devices. However, further improvements are needed in areas such as security, flexibility, and energy efficiency to enhance the effectiveness and adoption of these systems.

REFERENCES

1. Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, *78*, 641–658. https://doi.org/10.1016/j.future.2017.02.014

2. Wu, T., Wu, F., Redoute, J. M., & Yuce, M. R. (2017). An autonomous wireless body area network implementation towards IoT connected healthcare applications. *IEEE access*, *5*, 11413-11422.

3. Chen, X., Ma, M., & Liu, A. (2018). Dynamic power management and adaptive packet size selection for IoT in e-Healthcare. *Computers & Electrical Engineering*, *65*, 357-375.

4. Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2019). RETRACTED ARTICLE: An ontology-driven personalized food recommendation in IoT-based healthcare system. *The Journal of Supercomputing*, *75*(6), 3184-3216.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

5. Verma, P., Sood, S. K., & Kalra, S. (2018). Cloud-centric IoT based student healthcare monitoring framework. *Journal of Ambient Intelligence and Humanized Computing*, *9*(5), 1293-1309.
6. Yang, Y., Liu, X., & Deng, R. H. (2017). Lightweight break-glass access control system for healthcare Internet-of-Things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3610-3617.
7. Gupta, V., Singh Gill, H., Singh, P., & Kaur, R. (2018). An energy efficient fog-cloud based architecture for healthcare. *Journal of Statistics and Management Systems*, *21*(4), 529-537.
8. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *Ieee Access*, *6*, 20596-20608.
9. Ould-Yahia, Y., Banerjee, S., Bouzefrane, S., & Boucheneb, H. (2017). Exploring formal strategy framework for the security in IoT towards e-health context using computational intelligence. In *Internet of things and Big data technologies for next generation healthcare* (pp. 63-90). Cham: Springer International Publishing.
10. Gupta, P. K., Maharaj, B. T., & Malekian, R. (2017). A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. *Multimedia Tools and Applications*, *76*(18), 18489-18512.
11. Dehury, C. K., & Sahoo, P. K. (2016). Design and implementation of a novel service management framework for IoT devices in cloud. *Journal of Systems and Software*, *119*, 149-161.
12. Kumar, P. M., & Gandhi, U. D. (2018). A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers & Electrical Engineering*, *65*, 222-235.
13. Parthasarathy, P., & Vivekanandan, S. (2020). A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm. *International Journal of Computers and Applications*, *42*(3), 222-232.
14. Kim, S. H., & Chung, K. (2015). Emergency situation monitoring service using context motion tracking of chronic disease patients. *Cluster Computing*, *18*(2), 747-759.
15. Bhuvaneswari, G., & Manikandan, G. (2018). A novel machine learning framework for diagnosing the type 2 diabetics using temporal fuzzy ant miner decision tree classifier with temporal weighted genetic algorithm. *Computing*, *100*(8), 759-772.
16. Azimi, I., Anzanpour, A., Rahmani, A. M., Pahikkala, T., Levorato, M., Liljeberg, P., & Dutt, N. (2017). HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT. *ACM Transactions on Embedded Computing Systems (TECS)*, *16*(5s), 1-20.
17. Muhammed, T., Mehmood, R., Albeshri, A., & Katib, I. (2018). UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities. *IEEE Access*, *6*, 32258-32285.
18. Kumar, P. M., Lokesh, S., Varatharajan, R., Babu, G. C., & Parthasarathy, P. (2018). Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. *Future Generation Computer Systems*, *86*, 527-534.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal
National Research Journal

19. Xu, X., Fu, S., Qi, L., Zhang, X., Liu, Q., He, Q., & Li, S. (2018). An IoT-oriented data placement method with privacy preservation in cloud environment. *Journal of Network and Computer Applications*, *124*, 148-157.
20. Elmisery, A. M., Rho, S., & Aborizka, M. (2019). A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Cluster Computing*, *22*(Suppl 1), 1611-1638.
21. Zhou, W., & Piramuthu, S. (2018). IoT security perspective of a flexible healthcare supply chain. *Information Technology and Management*, *19*(3), 141-153.