

IoT-Driven Healthcare Communication: Real-Time Interactions, Security, and Ethical Considerations

Safa Hussein Oleiwi[1], ,Saraswathy Shamini Gunasekaran[2], Mazin Abed Mohammed3, Karrar Ibrahim AbdulAmeer[4], ˒Moamin A. Mahmoud[5]

[1]College of Computing and Informatics, University Tenaga Nasional (UNITEN), Kajang 43000, Malaysia.
College of Education for humanities, Kerbala university, Iraq.
safa.h@uokerbala.edu.iq
[2]College of Computing and Informatics, University Tenaga Nasional (UNITEN), Kajang 43000, Malaysia
SShamini@uniten.edu.my
[3]College of Computer Science and Information Technology, University of Anbar, Iraq
mazinalshujeary@uoanbar.edu.iq
[4]College of Information Technology Engineering, Al-Zahraa University for Women, Iraq
Karrar.ibrahim@alzahraa.edu.iq
[5]College of Computing and Informatics, University Tenaga Nasional (UNITEN), Kajang 43000, Malaysia
moamin@uniten.edu.my

ABSTRACT

The integration of Internet of Things (IoT) technologies into healthcare has revolutionized communication between patients, providers, and healthcare organizations. This paper explores how IoT enables real-time interactions, enhances patient engagement, and transforms data sharing in the healthcare sector. While addressing critical challenges like security and data privacy, the study emphasizes the ethical implications of IoT-driven communication in healthcare settings. By analysing various latency reduction and security improvement techniques, this survey offers insights into the role of IoT in shaping the future of connected healthcare.. In this context, latency issues include computational, communication (service), and network latencies. Real-time applications require low network, service, and compute latencies, and high secure which IoT must provide if it is to succeed. Ineffective communication can be hindered by factors such as network latency, which causes unwanted delays in message transmission. Accessing data via traditional cloud models is frequently impractical for real-time data-dependent services. In addition, traditional cloud computing paradigms frequently fail to meet the stringent quality-of-service (QoS) requirements of IoT devices. Still in their infancy, study on latency and safe techniques is in its inception, therefore, this paper investigates novel techniques for mitigating latency when transmitting time-sensitive data in real-time for cloud and IoT devices as well as improve security. By systematically evaluating these methods and technologies, this study serves as a valuable resource for academics and businesses seeking to identify latency-minimization techniques and improve security. In addition, the paper explores emerging study trends and technical distinctions between diverse technologies and methodologies. In light of the growing interest in latency minimization and its critical importance for time-sensitive apps, this study reviews and synthesises current approaches, tools, challenges, and techniques within the context of IoT and cloud. It classifies these methods, identifies extant gaps as well as challenges, and provides insight for future study. This paper will explore how IoT technology transforms healthcare communication by enabling real-time interactions between patients and healthcare providers, enhancing the accessibility and immediacy of health-related information. Ultimately, this paper sets the groundwork for future study by identifying critical unresolved issues that will steer the development of this field.

Keyword: - IoT, QoS, healthcare, Security, Network latency, IoMT.

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has transformed healthcare communication by enabling real-time interactions between patients and healthcare providers. This transformation has significant implications for the accessibility, immediacy, and quality of health-related information delivery. As IoT devices generate massive data streams, they create new opportunities for enhanced patient engagement and better decision-making. However, these opportunities come with challenges such as maintaining data privacy and ensuring secure communication channels. This paper explores how IoT technology not only addresses latency and security challenges but also redefines the communication dynamics within the healthcare industry [1, 2].

This data deluge has a significant impact on cloud-based services that rely on the timely transmission of real-time data, which is one of the most significant concerns resulting from it. As the volume of data transmission increased, so did the likelihood of errors, demonstrating a direct correlation between data size and error occurrence. This phenomenon is observed in the form of packet loss and transmission latency, both of which are closely associated with the transmission of data from Internet of Things (IoT) devices to cloud servers. End-users experienced a decrease in quality of service (QoS) as a result [3]. The overwhelming volume of data generated by Internet of Things (IoT) devices presented end-users with significant difficulties in coping with exceptionally lengthy transmission delays and inadequate services. The excessive rainfall imposed a significant strain on the cloud computing infrastructure [4].

A significant outcome resulting from elevated service latency was the emergence of a synchronisation issue between client requests and server responses, resulting in a minimal service delay. Communication issues between Internet of Things (IoT) devices and the cloud were substantially exacerbated by the presence of network congestion. Within the realm of real-time services, the problem of excessive service latency has emerged as the leading cause of delays. The number of gateway nodes required to facilitate the transmission of data packets is directly proportional to the geographical distance between Internet of Things devices and their endpoints. This increase in gateway nodes adds complexity and latency to the ecosystem as a whole [5].

The substantial obstacles posed by data volume, transmission latency, and service synchronisation had a significant impact on the efficacy of cloud-based services dependent on real-time data. These obstacles had a substantial impact on the overall efficacy of these services. The resolution of these issues would be of the utmost significance for ensuring the continued growth and effectiveness of Internet of Things (IoT) applications and services. Figure 1 illustrates the integration of Internet of Things (IoT) technology with healthcare applications.

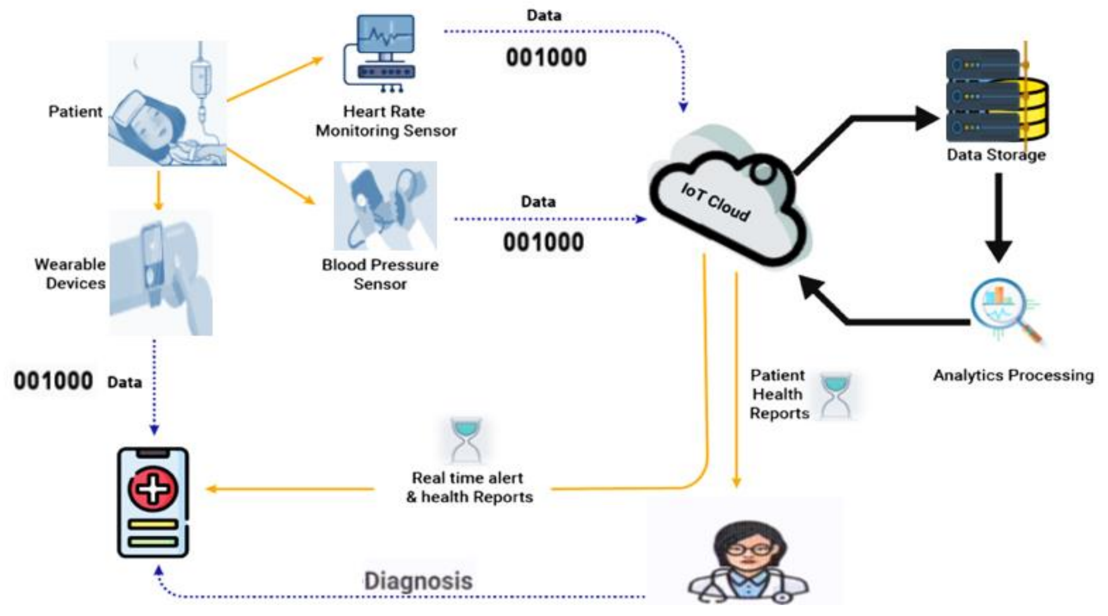

Fig. 1: IoT in Healthcare Apps.

2. RELATED WORK

Previous studies have largely focused on the technical aspects of IoT in healthcare, such as latency reduction and security enhancements. However, there is a growing need to understand how IoT facilitates communication within healthcare networks. Research has shown that IoT devices, such as wearable health monitors and telemedicine platforms, have improved the way healthcare providers interact with patients. For instance, IoT-enabled devices facilitate real-time monitoring of patient conditions, allowing for prompt medical intervention. This section reviews the integration of IoT with communication platforms like mobile health applications, emphasizing their role in enhancing healthcare communication networks. Figure 2 illustrates the procedural framework of integrating blockchain technology within IoT healthcare system.

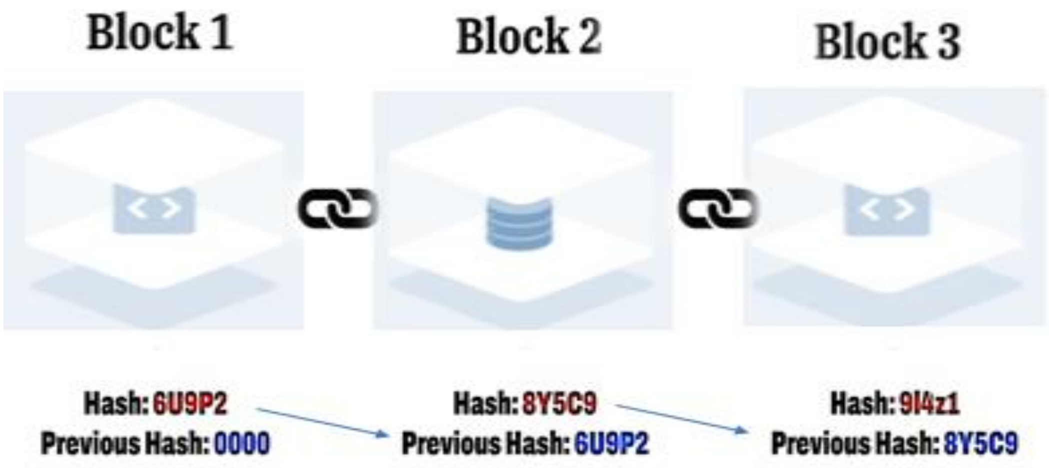

Fig. 2: Process of blockchain in IoT healthcare system

In study [6], a patient healthcare programme designed to increase energy efficiency was presented. This scheme also included certificate-based security measures, which were implemented to safeguard remote healthcare services. At [7] and [8] suggested the use of energy-efficient machine learning techniques that incorporate supervised labelling in order to address the problem of dynamic intrusion threats. These approaches were designed specifically for mobile Android cloud-based healthcare applications. The methodologies were developed with the objective of optimising the application processing procedure within the blockchain-powered network. The purpose of these methodologies is to address the inherent problems with authentication and authorization that arise when dealing through data of patient. These investigations effectively addressed security as well as energy consumption issues, particularly in relation to network-edge administering devices. Nevertheless, it is essential to highlight that the study mostly concentrated on the examination of security measures as well as energy consumption inside centralised healthcare apps. When confronted with a large number of diverse nodes in the healthcare industry, this method frequently resulted in an excessive use of resources and an increase in security vulnerabilities.

In order to resolve these limitations, a number of studies [9–12] have proposed a decentralised healthcare system employing blockchain technology in tandem with the Internet of Things (IoT). Using a decentralised method, the primary objective was to mitigate security vulnerabilities associated with centralised healthcare Internet of Things (IoT) systems. Utilising public blockchain technologies facilitated the processing of public healthcare data, ensuring data integrity across heterogeneous groups while simultaneously reducing energy consumption relative to centralised solutions. Nonetheless, the inherent limitations of blockchain technology, specifically its capacity to manage large datasets on nodes, posed obstacles to achieving accurate governance over these healthcare systems in terms of security and energy efficiency.

In response to these issues, the studies [13,14] has proposed blockchain-based healthcare system solutions that prioritise delay optimisation and energy efficiency. The aforementioned advancements prioritised the reduction of processing delays in healthcare data transmission between fog and cloud nodes through the utilisation of dynamic scheduling algorithms and machine learning techniques. In spite of the implemented optimisations, the training and testing of models within consensus blocks caused delays in the final decision-making process for numerous studies.

Additional progress was made in studies [15–18], which included the proposal of a healthcare system propelled by federated learning, as well as the incorporation of trivial offloading as well as scheduling systems. By implementing smart-agreement regulations, primary objectives of these solutions were to reduce delays, enhance security measures, and optimise energy consumption. The use of machine learning techniques for outsourcing and adaptive scheduling was crucial to the efficient management of healthcare data within fog-cloud networks.

Recent study has shown the emergence of innovative healthcare systems that integrate adaptive and artificial intelligence-driven mechanisms to augment security, privacy, and energy efficiency within the realm of blockchain technology [18–21]. These platforms were designed with the objective of predicting security as well as energy risks in the IoT network through the use of several mining techniques, including proof of stake (PoS), proof of work (PoW), as well as Byzantine disappointment, for the purpose of authenticating and anticipating network nodes. The previously listed blockchain frameworks, specifically Ethereum, Fabric, Corda, and IBM, have made significant advancements in the field of decentralised security. Nevertheless, scholarly study has emphasised the importance of validating data on the client side in the context of offloading and local processing.

Table 1 provides a comprehensive for the most important study that has been examined, encompassing the implemented application, the proposed methodology, the security challenges encountered, and the outstanding issues that remain unresolved. Additionally, the table outlines the objectives that were set for each study, and whether they were achieved. The year in which each problem was resolved is also specified, enabling identification of the unresolved issues.

Table 1: Comprehensive study of the implemented application, recommended methods, security challenges and objectives; that must be focused on.

Ref.	**Implement App**	**Methodology**	**Security Challenges**	**Objectives**	**Year**
[22]	System for Managing and Sharing Medical Records	Identification of unknown key exploiters	Concerning the confidentiality, integrity, availability, and privacy of data	Development of a Distributed Ledger Technology (DLT)-based Data Management Platform	2020
[23]	RPM (Remote Patient Medicine) and Telemedicine	Dedicated to bridging the gap between the blockchain platform concept and the healthcare industry	Data collecting, patient monitoring, and privacy and data security	Safe and reliable RPM using the blockchain	2021
[24]	The EHR System, or Electronic Health Record	Consider population-level data collection as an example of a work that could benefit from blockchain automation that could be of use to healthcare practitioners.	Safety, distribution, accessibility, and integrity of data	E.H.R security as well as usability improved by employing blockchain technology.	2021
[25]	Data storage & Security	Dedicated to improving the technological advantages of blockchain applications, for example by coordinating Internet of Things gadgets.	Safety, Authorization, Reliability, as well as Transfer of Data	Creating Safe Methods of Data Transmission as well as Storage	2022

[26]	Data analysis, computation on the edge and in the cloud	The human body generates one-of-a-kind protocols as a transmission channel as part of its efforts to construct a blockchain-based, decentralized social network.	Problems with information safety, administration, dependability, accuracy, manipulation, communication delays, and allocation of scarce resources.	Better decisions may be made when blockchain technology is combined with other processing of data platforms, like cloud as well as edge computing.	2023

3. IOT-IOMT AND APPLICATIONS IN MEDICAL DOMAIN

Figure 3 presents a schematic representation of the barriers that hinder the general adoption and utilisation of the Internet of Medical Things (IoMT). Therefore, we discuss various studies contributions to the field of IoT have informed the selection of the applications under consideration. The papers were selected from authoritative databases including those maintained by ACM, IEEE, and Elsevier using established criteria for acceptance or rejection. We have taken into account the most up-to-date IoT applications in the medical field. The purpose of this study was to catalogue the different healthcare applications of IoT technology.

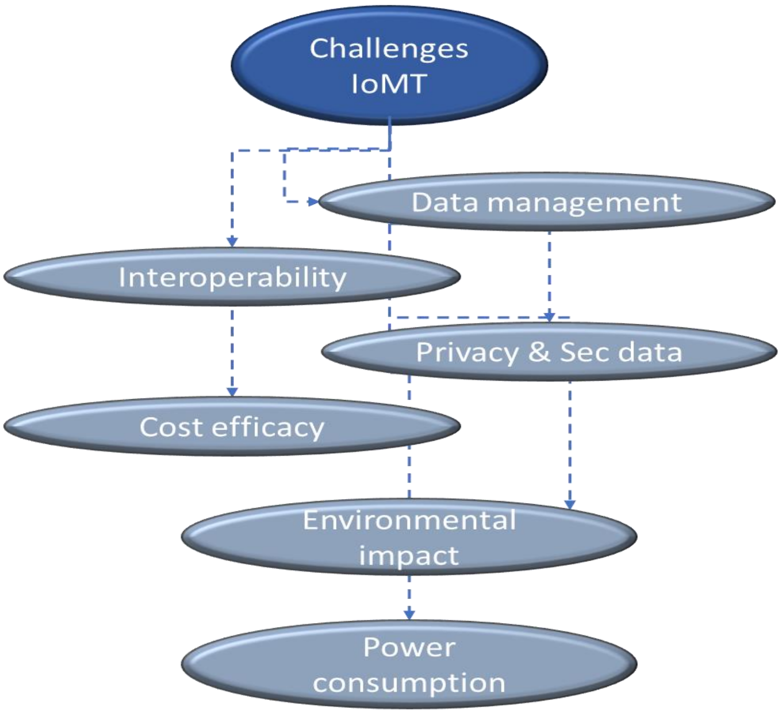

Fig. 3: A schematic depiction of the challenges to IoT use.

Table 2 presents a comprehensive summary of diverse study investigations conducted in the domain of IoT applications within the healthcare sector, specifically focusing on the Internet of Medical Things (IoMT) .

Table 2: Overview of various studies in the field of IoT-IoMT.

Ref.	Application Description	Solutions and Problems Solved	Algorithms/Methods Used
[27]	Integration of CoAP for the deployment of healthcare devices; performance comparison with HTTP and	**Solutions:** Enhanced deployment of healthcare devices in IoT environments.	CoAP, HTTP, JSON, XML

	CoAP; evaluation of packet volume, loss rate, and syntax (JSON vs. XML).	**Problems Solved:** Enhanced gearbox efficacy and quality of service. Performance comparison of CoAP and HTTP	
[28]	Monitoring patient posture with a specially designed mattress and Cohen's Coefficient to reduce storage and computational costs.	Solutions: Precise patient posture monitoring Problems Solved: Enhanced monitoring accuracy, reduced storage, and computational costs.	Cohen's Coefficient
[29]	Construction of the MNS with IoT architecture and multiple technologies for accurate medication dispensing.	Solutions: Facilitated precise medication dispensation **Problems Solved: Improved medication accuracy and administration efficiency.**	Bluetooth, 2G-3G, WSN, RFID, ZigBee, and Wi-Fi
[30]	Development of a rehabilitation system using SOA, IoT technologies, optimisation methods, resource allocation, and ontology for diagnostics	Solutions: Enhanced rehabilitation processes and knowledge exchange. **Problems Solved:** Improved rehabilitation efficiency	SOA, IoT, optimization methods, ontology
[31]	Examining the relationship between m-health, M2M, and 5G technologies in order to address mobile health concerns.	Solutions: Leveraging emerging technologies for mobile health solutions **Problems Solved:** Potential for resolving m-health issues	M2M, 5G technologies
[32]	Introduction of an intelligent system for diagnosing Parkinson's disease and assisting with medical care in residential settings.	Solutions: Support for physicians in various aspects of medical care for Parkinson's disease **Problems Solved:** Enhanced treatment, prescription, diagnosis, rehabilitation, and monitoring.	Intelligent monitoring, decision support
[33]	IoT capabilities in medical care, with a particular emphasis on upcoming 4G health applications with IPV6 connectivity	Solutions: Utilization of IoT and medical health for 4G health applications **Problems Solved:** Potential for advanced 4G health applications	IoT, IPV6 connectivity
[34]	Emphasis on message transmission and timing coordination in the design of a low-cost IoT-based medical sensing device for physiological monitoring.	Solutions: Low-cost, IoT-based physiological monitoring **Problems Solved:** Efficient message transmission and timing coordination	Message transmission optimization
[35]	Using semantic approaches and cloud-based solutions to address IoT data preservation issues.	Solutions: IoT data preservation with semantic and cloud-based approaches **Problems Solved:** Addressed IoT data preservation challenges.	Semantic approaches, cloud-based solutions
[36]	addressing obstacles in patient identification within health monitoring systems, with a focus on noise reduction and precision improvement.	Solutions: Improved patient identification. **Problems Solved:** Noise reduction, accuracy enhancement in patient identification	Noise reduction techniques, accuracy enhancement methods
[37]	Presentation of fundamental solutions for IoT-based services	Solutions: Fundamentals for IoT-based services	IoT principles, data engineering

	in data engineering and IoT principles	**Problems Solved:** Provided foundational knowledge for IoT-based services.	
[38]	Introduction of an automated system for monitoring autistic individuals, using individualised sensors to monitor cerebral signals.	Solutions: Automated monitoring of individuals with autism. **Problems Solved:** Efficient and personalized monitoring.	Automated monitoring, personalized sensor technology
[39]	Utilisation of FPGA technology for CAD algorithm development in kidney ultrasound image abnormality detection.	Solutions: FPGA-based CAD algorithm for kidney ultrasound abnormalities. **Problems Solved:** Improved detection accuracy.	FPGA, CAD algorithm
[40]	Multiple implementation modules comprise a cloud-based infrastructure for medical healthcare monitoring that is hosted in the cloud.	Solutions: Cloud-based medical healthcare monitoring framework. **Problems Solved:** Enhanced healthcare monitoring implementation.	Cloud computing, modular framework
[41]	Focusing on ECG wave monitoring, an Android app will be developed for the healthcare industry utilising IoT and cloud computing technologies.	Solutions: Android app for ECG wave tracking in healthcare **Problems Solved:** Integration of IoT and cloud for healthcare apps.	Android app development, IoT integration
[42]	Developing a tool to monitor patients' health by measuring their heart rate with smart health bands and sending messages based on heart rate values.	Solutions: Health monitoring using heart rate measurements **Problems Solved:** Enhanced patient monitoring and communication.	Heart rate measurement, smart health bands
[43]	Design and architectural design for a smart hospital employing IoT technology to improve overall hospital administration.	Solutions: IoT-based smart hospital system for improved information management. **Problems Solved:** Efficient hospital system management.	IoT architecture, smart hospital design
[44]	IoT-based medical monitoring system for monitoring geriatric patients continuously	Solutions: Continuous patient monitoring with IoT-based system **Problems Solved:** Enhanced patient care.	IoT-based patient monitoring
[45]	A novel method for monitoring patients with OSA.	Solutions: Novel methodology for OSA monitoring. **Problems Solved:** Improved patient monitoring for sleep disorders.	Novel monitoring methodology
[46]	Utilising RFID technology to develop an IoT-based electronic healthcare unit paradigm for India based on health statistics.	Solutions: IoT-based healthcare unit for digitizing Indian medical units **Problems Solved: :** Enhanced healthcare data digitization	RFID technology, healthcare unit model
[47]	iCarMa is a presentation of a methodology for early risk indicators in cardiac patients using IoT.	Solutions: Early risk indications for cardiac patients. **Problems Solved:** Improved cardiac patient monitoring	iCarMa methodology

4. CHALLENGES AND BENEFITS OF IOT IN HEALTHCARE

The IoT has become a significant and influential factor in the healthcare industry, offering a variety of benefits that can enhance patient care, operational efficiency, and medical research. This technology has the ability to remotely monitor patients' vital signs and chronic conditions, thereby providing healthcare providers with real-time data for improved decision-making and prompt intervention. Moreover, the IoT facilitates the efficient administration of resources by improving the distribution of hospital beds, equipment, and personnel, resulting in both financial benefits and improved patient care quality. The vast amount of data generated by IoT devices also contributes to data analytics, facilitating the identification of health patterns and enabling the conduct of groundbreaking research. Moreover, the IoT plays a crucial role in facilitating medication management through multiple mechanisms, such as sending patients reminders for timely drug consumption, reducing the occurrence of errors, and increasing adherence to prescribed treatment programs. Additionally, it facilitates emergency response by employing peripheral devices capable of detecting falls and alerting caregivers or emergency personnel immediately. In addition, the use of IoT technology has increased the accessibility of telemedicine, thereby facilitating the delivery of healthcare services to geographically isolated or underserved regions.

Integration of IoT technology into the healthcare industry is not, however, without obstacles. The primary concern revolves around security and privacy, given the utmost need of safeguarding sensitive patient information from potential cyber threats. IoT devices are susceptible to cyberattacks, which can pose a serious threat to the confidentiality of medical records. Due to the heterogeneous communication protocols employed by various IoT devices, interoperability issues arise, impeding the seamless integration of these devices into existing healthcare systems. The vast amount of data generated by these devices may impose a significant burden on healthcare systems, making it difficult to extricate valuable insights and effectively manage the information flood. Due to the necessity of regulatory compliance, the deployment of IoT is accompanied by increased complexity and financial burden, particularly in relation to stringent standards such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. The maintenance of dependability and precision in IoT devices is crucial for ensuring the safety of patients, as the presence of inaccurate data may lead to erroneous decisions. In addition, senior citizens' approval and utilization of digital devices can pose a significant obstacle to the implementation of patient adoption strategies. Lastly, there are ethical dilemmas regarding patient consent, data ownership, and the possibility of discriminatory practices resulting from health data. In order to completely realize the IoT potential within the healthcare industry, it is essential to effectively address these issues and capitalize on its benefits. Figure 4 and Figure 5 illustrates the challenges and benefits associated with the implementation of the IoT in healthcare applications.

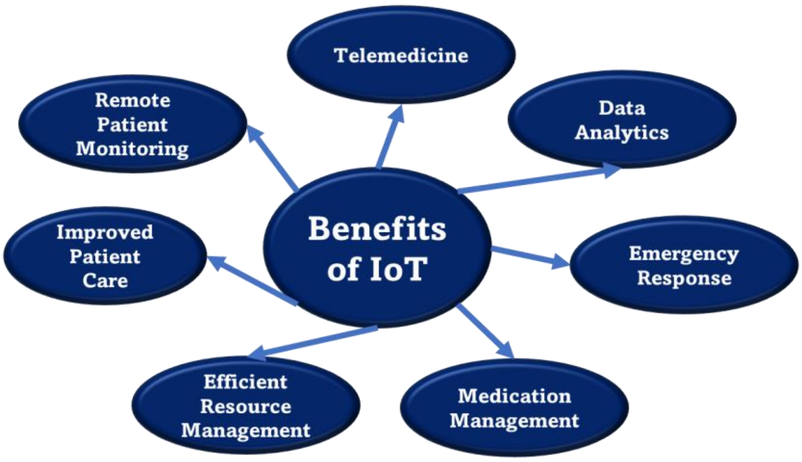

Fig. 4: Benefits of Internet of Things (IoT) in Healthcare Applications

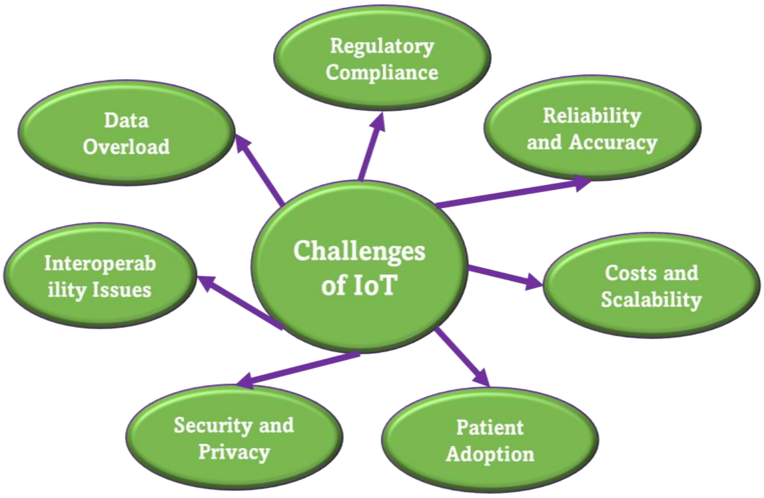

Fig. 5: Challenges of Internet of Things (IoT) in Healthcare Applications

4.1. Challenges of Internet of Thing in Healthcare Applications

Following a preliminary investigation, we have identified several noteworthy obstacles within the realm of the IoT. It is our contention that addressing these challenges within the realm of IoT has the potential to increase the IoT standard implementation within the medical care domain. The IoT has the potential to enhance the quality and dependability of medical healthcare services.

Internet communication has undergone a significant transformation due to the IoT's introduction. This innovation has played a crucial role in the advancement of numerous challenging fields, particularly in the field of medical technology. One of the primary rationales for bridging the divide between medical practitioners, individuals seeking medical attention, and healthcare facilities is the facilitation of streamlined, precise, and adaptable healthcare services. The implementation of IoT technology in healthcare settings has facilitated the ability of medical professionals and hospital personnel to perform their duties with greater accuracy and efficiency, while also reducing the cognitive demands of their tasks.

The Challenges have been chosen based on the contributions of various scientists in the field of internet of thing from diverse sources. The articles were selected from reputable repositories such as ACM, IEEE, and Elsevier based on predetermined criteria for acceptance and rejection. We have incorporated the latest challenges pertaining to the IoT within the healthcare sector. The objective was to enumerate the obstacles associated with the implementation of IoT technology in the medical healthcare sector. As explain in the Table 3.

Table 3: Challenges of IoT in the domain of medical healthcare.

Ref.	Challenges
[22]	Storage space available on the system's CPU limited by network factors such as bandwidth
[48]	Diverse device management Size, data volume, and processing speed Application, adaptability and development Security of Personal Information Medical Knowledge
[49]	Data exchange the availability of assets Privacy
[23]	Problems with hardware implementation and design optimization
[50] , [49], [55], [56]	Challenges of Security

[49], [54], [52]	Interoperability
[51]	Modelling the relationship between acquired measurements and maladies presents technical difficulties.
[48]	Medical Care by Intelligent.
[54]	Real time processing System consistency low electrical consumption
[54], [52]	Integration of Data
[53]	Unstructured, expanding, and heterogeneous data at an exponential rate

4.2. Benefits of Internet of Thing in Healthcare Applications

The Internet of Thing confers numerous benefits that can be derived by individuals, society, the environment, customers, and enterprises. However, like any technology, it also entails certain drawbacks alongside its advantages. Table 2.5 presented enumerates the primary advantages derived from IoT; it's has proven to be highly advantageous in the field of medical healthcare. The advent of IoT-based applications and systems has brought about a transformation in the world that was once only imagined by individuals in the 1990s. The emergence of the IoT has resulted in a substantial revolution in the domain of internet communication. The progress has significantly contributed to the progress of numerous complex disciplines, namely within the realm of medical technology. One of the primary rationales for bridging the divide among physicians, patients, and healthcare services is the facilitation of streamlined precise, and adaptable medical care. The implementation of IoT technology in healthcare facilitates the ability of medical professionals and hospital personnel to perform their duties with greater precision and efficiency, while also reducing the cognitive load required to complete tasks. The Table 4 of applications serves as evidence for this claim. The incorporation of IoT technology in the medical domain has yielded remarkable benefits for patients, owing to its user-friendly nature.

Table 4: Benefits of IoT in the domain of medical healthcare.

Ref.	**Benefits**
[54]	1. Facilitate ease of living 2. Cost-effective health care 3. Patient outcome is enhanced. 4. In real time, diseases are managed. 5. The Standard of Living Raises 6. The final product is better for the user. 7. Enhanced patient care 8. saving money 9. control and avoidance 10. Monitored. etc.
[57]	Timely dosing of medication Family members will be included in patient care plans.
[58]	Energy efficiency, such as time, money, etc.
[59]	1. Simpleness 2. Affordability 3. Facilitated use
[60]	IoT-based healthcare for doctors' off-hours shifts.
[61]	Medical records can be conveniently managed by doctors.

The selection of advantages is based on the work of many experts in the field of IoT study. The articles came from authoritative sources including ACM, IEEE, and Elsevier, and were chosen using strict criteria. Our evaluation takes into account the most up-to-date information regarding the positive effects of IoT in the medical field. There has been a growing need to highlight the benefits of IoT for medical care as a result of its rapid development and proliferation. The goal was to list the benefits of IoT.

5. Ethical Communication Considerations

The integration of IoT in healthcare introduces complex ethical challenges, particularly regarding data privacy, patient consent, and the responsible sharing of sensitive health information. As IoT devices collect and transmit vast amounts of data, ensuring the confidentiality and integrity of patient information becomes paramount. This section explores the ethical considerations surrounding IoT-driven communication in healthcare, focusing on data privacy, informed consent, and trust-building between patients and providers.

5.1. Data Privacy and Security Concerns

Data privacy is a critical issue when using IoT devices in healthcare. IoT devices often gather real-time patient data, including vital signs and medical histories, which are transmitted to healthcare providers and stored on cloud-based platforms. The sensitivity of this data necessitates robust security measures to prevent unauthorized access and breaches. According to [63]. (2023), one of the primary vulnerabilities in IoT-based healthcare systems is their susceptibility to cyberattacks, which can compromise patient privacy and data integrity. Protecting this data requires implementing encryption methods and secure communication protocols to ensure that patient information remains confidential during transmission and storage.

5.2. Ethical Implications of Data Sharing

The sharing of patient data across different platforms and with multiple stakeholders such as healthcare providers, insurers, and research institutions poses ethical dilemmas. While data sharing can improve healthcare outcomes through better collaboration and research opportunities, it also risks exposing sensitive information to parties beyond the patient's control. According to [63]. (2024), data sharing should be guided by strict ethical frameworks that prioritize patient autonomy and respect for privacy. Such frameworks should include consent-based data sharing agreements and anonymization techniques to protect patient identities when data is used for research or shared with third parties.

6. CONCLUSION

This survey highlights the transformative impact of IoT on healthcare communication, emphasizing how real-time interactions and enhanced data sharing can improve patient outcomes. While IoT technologies present solutions for latency reduction and data security, they also pose challenges related to ethical data management and patient privacy. The study concludes that the future of connected healthcare lies in balancing the technological advantages of IoT with the need for secure and ethical communication practices, thereby ensuring trust and efficacy in healthcare delivery. The purpose of this paper was to provide a comprehensive examination of the major themes, technologies, and research directions in this field. During our investigation, we highlighted the numerous benefits that the IoT provides to the healthcare industry, including remote patient monitoring, improved healthcare delivery, streamlined resource allocation, and data analysis. The aforementioned innovations have the potential to fundamentally transform healthcare delivery, thereby improving patient outcomes and maximizing operational efficiency. The IoT poses significant challenges to the healthcare industry. IoT issues include security and privacy, interoperability hurdles, and the efficient management of the vast amount of data generated by IoT devices. The difficulties posed by regulatory compliance and the need to ensure the dependability and accuracy of these devices are formidable obstacles that demand careful consideration. Moreover, our investigation centered on the dynamic domain of latency reduction strategies and security measures in the regions of the IoT and cloud computing. In order to meet the needs of time-sensitive applications, we acknowledged the significance of overcoming latency obstacles effectively. Upon completion of this survey, it is evident that the integration of the IoT into the healthcare sector is fundamentally transforming the industry. Relevant parties must navigate the complex landscape of data security, interoperability, and regulatory conformance in order to effectively utilize the capabilities of the IoT in the healthcare sector. Concurrently, these stakeholders must persevere in their endeavors to develop and improve IoT applications.

REFERENCES

[1] Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., Khoukhi, L.: IoT technologies for smart cities. IET Netw. 7(1), 1–13 (2017)

[2] Wortmann, F., Flu¨chter, K.: Internet of things. Bus. Inf. Syst. Eng. 57(3), 221–224 (2015)

[3] Shukla, S., Hassan, M.F., Khan, M.K., Jung, L.T., Awang, A.: An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PLoS ONE 14(11), e0224934 (2019)

[4] Brogi, A., Forti, S.: QoS-aware deployment of IoT applications through the fog. IEEE Internet Things J. 4(5), 1185–1192 (2017).

[5] Alicherry, M., Lakshman, T.: Optimizing data access latencies in cloud systems by intelligent virtual machine placement. In: 2013 Proceedings IEEE INFOCOM. IEEE, pp. 647–655 (2013)

[6] S. Abirami, P. Chitra, Energy-efficient edge based real-time healthcare support system, in: Advances in Computers, vol. 117, (1) Elsevier, 2020, pp. 339–368.

[7] T. Saba, K. Haseeb, I. Ahmed, A. Rehman, Secure and energy-efficient framework using internet of medical things for e-healthcare, J. Inf. Public Health 13 (10) (2020) 1567–1575.

[8] N. Singh, A.K. Das, Energy-efficient fuzzy data offloading for IoMT, Comput. Netw. 213 (2022) 109127.

[9] A.H. Sodhro, M.S. Al-Rakhami, L. Wang, H. Magsi, N. Zahid, S. Pirbhulal, K. Nisar, A. Ahmad, Decentralized energy efficient model for data transmission in IoT-based healthcare system, in: 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), IEEE, 2021, pp. 1–5.

[10] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.

[11] J.J. Kang, M. Dibaei, G. Luo, W. Yang, P. Haskell-Dowland, X. Zheng, An energy-efficient and secure data inference framework for internet of health things: a pilot study, Sensors 21 (1) (2021) 312.

[12] A. Sharma, R. Tomar, N. Chilamkurti, B.-G. Kim, Blockchain based smart contracts for internet of medical things in e-healthcare, Electronics 9 (10) (2020) 1609.

[13] H.S. Anbarasan, J. Natarajan, Blockchain based delay and energy harvest aware healthcare monitoring system in WBAN environment, Sensors 22 (15) (2022) 5763.

[14] L. Liu, Z. Li, Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things, Ieee Access 10 (2022) 53640–53651.

[15] A. Lakhan, M.A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, W. Wang, Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare, IEEE J. Biomed. Health Inf. (2022).

[16] M.A. Dootio, F. Alqahtani, I. R Alzahrani, F. Baothman, S.Y. Shah, S.A. Shah, N. Anjum, Q.H. Abbasi, M.S. Khokhar, et al., Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network, Electronics 10 (16) (2021) 1974.

[17] M.A. Mohammed, A.N. Rashid, S. Kadry, T. Panityakul, K.H. Abdulkareem, O. Thinnukool, Smart-contract aware ethereum and client-fog-cloud healthcare system, Sensors 21 (12) (2021) 4093.

[18] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, M. Xu, EEDTO: an energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing, IEEE Internet Things J. 8 (4) (2020) 2163–2176.

[19] S. Singh, D. Kumar, Energy-efficient secure data fusion scheme for IoT based healthcare system, Future Gener. Comput. Syst. (2023).

[20] S. Jain, R. Doriya, Security framework to healthcare robots for secure sharing of healthcare data from cloud, Int. J. Inf. Technol. (2022) 1–11.

[21] V. Pawar, S. Sachdeva, ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain, Int. Trans. Oper. Res. (2023).

[22] Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020, July). A blockchain based secured healthcare framework. In 2020 International Conference on Computational Performance Evaluation (ComPE) (pp. 386-391). IEEE.

[23] Hemalatha, P. Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology. Turk. J. Comput. Math. Educ. 2021, 12, 2554–2561.

[24] Singh, C., Chauhan, D., Deshmukh, S. A., Vishnu, S. S., & Walia, R. (2021). Medi-Block record: Secure data sharing using block chain technology. Informatics in Medicine Unlocked, 24, 100624.

[25] CHELLADURAI, M. U., Pandian, S., & Ramasamy, K. (2021). A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. Health Policy and Technology, 10(4), 100513.

[26] Verdonck, M., & Poels, G. (2020). Decentralized data access with IPFS and smart contract permission management for electronic health records. In Business Process Management Workshops: BPM 2020 International Workshops, Seville, Spain, September 13–18, 2020, Revised Selected Papers 18 (pp. 5-16). Springer International Publishing.

[27] Albahri, A., Alwan, J. K., Taha, Z. K., Ismail, S. F., Hamid, R. A., Zaidan, A., Albahri, O., Zaidan, B., Alamoodi, A., & Alsalem, M. (2021, January). IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. Journal of Network and Computer Applications, 173, 102873. https://doi.org/10.1016/j.jnca.2020.102873

[28] Kaczmarczyk, A., Zając, P., & Zabierowski, W. (2022, June 23). Performance Comparison of Native and Hybrid Android Mobile Applications Based on Sensor Data-Driven Applications Based on Bluetooth Low Energy (BLE) and Wi-Fi Communication Architecture. Energies, 15(13), 4574. https://doi.org/10.3390/en15134574

[29] Pillai, A. S., Chandraprasad, G. S., Khwaja, A. S., & Anpalagan, A. (2021, June). A service oriented IoT architecture for disaster preparedness and forecasting system. Internet of Things, 14, 100076. https://doi.org/10.1016/j.iot.2019.100076

[30] Waghmare, M., Antapurkar, H., & Wagh, M. S. (2022). I-Health-Care: Technologies towards 5G Network for Intelligent Health-Care Using IoT Notification with Machine Learning Programming. SSRN Electronic Journal.

[31] Mohsin, A., Zaidan, A., Zaidan, B., Albahri, O., Albahri, A., Alsalem, M., & Mohammed, K. (2019, May). Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Computer Standards & Interfaces, 64, 41–60. https://doi.org/10.1016/j.csi.2018.12.002

[32] Thematic Dynamics of Internet of Things (IoT): Impact on Digital Personalized Healthcare (PHC). (2021, July 19). International Journal of Women's Health Care, 6(3). https://doi.org/10.33140/ijwhc.06.03.05

[33] Sun, Z., Zhu, M., & Lee, C. (2021, September 19). Progress in the Triboelectric Human–Machine Interfaces (HMIs)-Moving from Smart Gloves to AI/Haptic Enabled HMI in the 5G/IoT Era. Nanoenergy Advances, 1(1), 81–121. https://doi.org/10.3390/nanoenergyadv1010005

[34] Gai, C., Shen, W., Yang, M., & Yu, J. (2023). PPADT: Privacy-Preserving Identity-Based Public Auditing with Efficient Data Transfer for Cloud-Based IoT Data. IEEE Internet of Things Journal, 1–1. https://doi.org/10.1109/jiot.2023.3282939

[35] Alshehri, F., & Muhammad, G. (2021). A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. IEEE Access, 9, 3660–3678. https://doi.org/10.1109/access.2020.3047960

[36] Singh, M. P., Aujla, G. S., & Bali, R. S. (2021, December). Blockchain for the Internet of Drones: Applications, Challenges, and Future Directions. IEEE Internet of Things Magazine, 4(4), 47–53. https://doi.org/10.1109/iotm.001.2100071

[37] Krasowicz, K., Michoński, J., Liberadzki, P., & Sitnik, R. (2020, June 6). Monitoring Improvement in Infantile Cerebral Palsy Patients Using the 4DBODY System—A Preliminary Study. Sensors, 20(11), 3232. https://doi.org/10.3390/s20113232

[38] El Moumni, S., Fettach, M., & Tragha, A. (2019, November). High throughput implementation of SHA3 hash algorithm on field programmable gate array (FPGA). Microelectronics Journal, 93, 104615. https://doi.org/10.1016/j.mejo.2019.104615

[39] Krishna, G., & Howard, S. (2021, December 22). How Yemen's healthcare

has been destroyed. BMJ, n3110. https://doi.org/10.1136/bmj.n3110

[40] Application of Android Mobile Platform in Remote Medical Monitoring System. (2018, May 6). International Journal of Recent Trends in Engineering and Research, 4(4), 598–607. https://doi.org/10.23883/ijrter.2018.4279.9x4ka

[41] Ali, M. M., Haxha, S., Alam, M. M., Nwibor, C., & Sakel, M. (2019, December 7). Design of Internet of Things (IoT) and Android Based Low Cost Health Monitoring Embedded System Wearable Sensor for Measuring SpO2, Heart Rate and Body Temperature Simultaneously. Wireless Personal Communications, 111(4), 2449–2463. https://doi.org/10.1007/s11277-019-06995-7

[42] Hospital Parking Management System using Internet of Things. (2023, January 1). Journal of Population Therapeutics and Clinical Pharmacology, 30(8). https://doi.org/10.47750/jptcp.2023.30.08.008

[43] Panwar, A. (2022). DEVELOPING AN ADVANCED MACHINE LEARNING AND INTERNET OF THINGS (IOT) BASED SYSTEM TO DEVISE AN EFFECTIVE HEALTHCARE MONITORING SYSTEM. INTERNATIONAL JOURNAL OF RESEARCH IN MEDICAL SCIENCES & TECHNOLOGY, 12(01), 228–237. https://doi.org/10.37648/ijrmst.v11i02.019

[44] Altintas, N., Fazlioglu, N., Guzel, S., Yilmaz, A., & Aydın, C. (2023, March 6). Is meteorin-like (Metrnl) a novel biomarker to distinguish patients with obstructive sleep apnea (OSA) and patients with OSA at vascular risk. Sleep and Breathing. https://doi.org/10.1007/s11325-023-02800-9

[45] Trivedi, H. S., & Patel, S. J. (2023, July). Homomorphic cryptosystem-based secure data processing model for edge-assisted IoT healthcare systems. Internet of Things, 22, 100693. https://doi.org/10.1016/j.iot.2023.100693

[46] Pal, M., Parija, S., Panda, G., Dhama, K., & Mohapatra, R. K. (2022, January 1). Risk prediction of cardiovascular disease using machine learning classifiers. Open Medicine, 17(1), 1100–1113. https://doi.org/10.1515/med-2022-0508

[47] Resta, M., Monreale, A., & Bacciu, D. (2021, August 17). Occlusion-Based Explanations in Deep Recurrent Models for Biomedical Signals. Entropy, 23(8), 1064. https://doi.org/10.3390/e23081064

[48] Liu, X., Ji, S., Wang, X., Liu, L., & Ren, Y. (2023, February 2). Blockchain Data Availability Scheme with Strong Data Privacy Protection. Information, 14(2), 88. https://doi.org/10.3390/info14020088

[49] Intelligent Customer-driven Solution for Pediatric Surgery Care for Parents and Their Children Undergoing Circumcision. (2019, November 22). Case Medical Research. https://doi.org/10.31525/ct1-nct04174404

[50] Albahri, O. S., Albahri, A. S., Mohammed, K. I., Zaidan, A. A., Zaidan, B. B., Hashim, M., & Salman, O. H. (2018, March 22). Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations. Journal of Medical Systems, 42(5). https://doi.org/10.1007/s10916-018-0943-4

[51] Subramanian, I., Verma, S., Kumar, S., Jere, A., & Anamika, K. (2020, January). Multi-omics Data Integration, Interpretation, and Its Application. Bioinformatics and Biology Insights, 14, 117793221989905. https://doi.org/10.1177/1177932219899051

[52] Shilpa, B. L., & Shambhavi, B. R. (2022, November 5). Structuring of Unstructured Data from Heterogeneous Sources. Indian Journal of Science and Technology, 15(41), 2188–2193. https://doi.org/10.17485/ijst/v15i41.1566

[53] Vadicherla, P., & Vadlakonda, D. (2021). Review on Security Issues and Challenges in Wireless Sensor Networks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3791578

[54] Digital Strategies for Big Picture Results. [Online]. Available: http://www.tcs.com/resources/white_papers/Pages/Internet-of-Things-Medical-Devices.aspx

[55] V. Tsoutsouras, D. Azariadi, K. Koliogewrgi, S. Xydis, and D. Soudris, “Software design and optimization of ECG signals analysis and diagnosis for embedded IoT devices,” in Components and Services for IoT Platforms, 2017.

[56] McGreevy, M. P. (2018, July 2). Housing Diversity and Affordability: The Effects of 35 Years of Exclusionary Land Use Regulations on Housing Affordability in Adelaide, South Australia. Urban Policy and Research, 1–18. https://doi.org/10.1080/08111146.2018.1476232

[57] LIU, S. (2023, May 15). The Security Challenges of The “Metaverse.” Security and Safety. https://doi.org/10.1051/sands/2023010

[58] McGreevy, M. P. (2018, July 2). Housing Diversity and Affordability: The Effects of 35 Years of Exclusionary Land Use Regulations on Housing Affordability in Adelaide, South Australia. Urban Policy and Research, 1–18. https://doi.org/10.1080/08111146.2018.1476232

[59] Fawzy, D., Moussa, S. M., & Badr, N. L. (2023, April). An IoT-based resource utilization framework using data fusion for smart environments. Internet of Things, 21, 100645. https://doi.org/10.1016/j.iot.2022.100645

[60] Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability. Healthcare Informatics Research, 26(1), 3. https://doi.org/10.4258/hir.2020.26.1.3

[61] Fritz, J., Wachira, J., Wilson-Barthes, M., Kafu, C., Chemutai, D., Wilson, I., Galarraga, O., & Genberg, B. (2022, July). EE251 Cost-Effectiveness of an Enhanced Patient Care (EPC) Intervention on Viral Suppression Among Adults Living with HIV in Kenya. Value in Health, 25(7), S383. https://doi.org/10.1016/j.jval.2022.04.499.

[62] Z. Abed, A. H. Shnawa, M. R. Hadi, K. Ibrahim, M. M. Adnan and W. Hameed, "Modeling of Metaheuristics with Deep Transfer Learning Based Visual Data Mining for the Healthcare Sector," 2023 6th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, 2023, pp. 629-635, doi: 10.1109/IICETA57613.2023.10351274.

[63] AL-inizi, M.S.M., Alzubaidi, Y.T., Oleiwi, S.H., Zahra, N.A.A., Yonan, J.F. (2024). Improvement Networks Intrusion Detection System Using Artificial Neural Networks (ANN). In: Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) Innovative Computing and Communications. ICICC 2024. Lecture Notes in Networks and Systems, vol 1021. Springer, Singapore. https://doi.org/10.1007/978-981-97-3591-4_43