iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63187

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Challenges with Medical Devices Connected To Hospital Network

Jagbir Singh
Robotics, Smith and Nephew

Abstract: ***The increasing adoption of connected healthcare technologies has transformed the traditional healthcare landscape, offering improved healthcare delivery. The combination of medical devices, sensors, and electronic health records has enabled real-time monitoring, remote care, and data-driven decision-making. However, the connectivity of medical devices to hospital network also introduces a vast array of challenges which include security challenges, scalability issues, and storage and interoperability issues. These challenges can compromise patient data, disrupt clinical workflows, and hinder the effective delivery of healthcare services. This article gives a detailed survey of the challenges and solutions in connected healthcare, with a focus on the technical and practical considerations of integrating medical devices into hospital networks. We explore the current state of connected healthcare, identify key challenges and limitations. Our analysis covers various aspects of connected healthcare, including device security, data privacy, network infrastructure, and standards for interoperability. Our paper also provides a comprehensive examination of the detailed architecture of connected healthcare system, encompassing different layers to facilitate a deeper understanding of connected healthcare system working. Finally, we explored the key research directions to handle the increasing challenges in connected healthcare system.***
Keywords: Medical Device Connectivity, HIPAA, Hospital Network, Patient data security.

I. INTRODUCTION

The increasing use of medical devices connected to the hospital network has revolutionized healthcare, enabling real-time monitoring, efficient data exchange, and improved patient care. This connectivity has brought about a significant transformation in the traditional healthcare system, enabling healthcare providers to access patient data remotely, track medical device performance, and receive alerts for potential issues [1]. The global market for connected medical devices is growing rapidly, projected to reach $94.2 billion by 2025, with the United States being a significant contributor to this growth [2].The growth of connected medical devices, such as bedside monitors, ventilators, and infusion pumps, has enabled healthcare providers to leverage advanced technologies like Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML) to improve patient outcomes with advanced data analytics and decision making. The adoption of connected medical devices has been driven by the need for improved patient care, reduced costs, and enhanced operational efficiency. For instance, connected patient monitors enable continuous vital sign monitoring, reducing the risk of adverse events. Moreover, connected medical devices have enabled remote patient monitoring, reducing hospital readmissions and saving hospitals significant cost [3]. During the COVID-19 pandemic, connected medical devices played a crucial role in enabling remote patient monitoring, reducing the burden on healthcare systems, and improving patient outcomes. For instance, connected ventilators and patient monitors enabled healthcare professionals to remotely monitor patients' vital signs, while telemedicine platforms enabled virtual consultations, reducing the risk of transmission and improving patient engagement. The increased connectivity has not only improved patient care but also generated significant revenue for healthcare providers, with the global telemedicine market alone projected to reach $286.22 billion by 2030 [4].

Despite the wide range of advantages offered by connected medical devices, their integration to the hospital network also introduces a complex array of technical, clinical, and operational challenges. One of the primary concerns is ensuring the security and integrity of patient data, as connected devices increase the risk of cyber-attacks and data breaches. Moreover, the integration of medical devices with electronic health records (EHRs) and other hospital systems poses technical challenges, such as ensuring compatibility and interoperability. This can lead to issues with data fragmentation, information blocking, and system crashes, which can have serious consequences for patient care. Additionally, connected medical devices produce enormous volumes of data, which can be overwhelming for healthcare professionals to manage. This leads to challenges in data analytics and interpretation, as well as issues with data quality, accuracy, and completeness. The huge quantity of data produced by connected devices can also lead to data overload, making it challenging for healthcare personnels to identify and respond to critical patient data in a timely manner.

Furthermore, the lack of standardization and interoperability between systems and devices causes problems with device integration, data sharing, and collaboration among healthcare teams. Overcoming these obstacles is essential to utilize the capabilities of connected medical devices and ensuring their safe and effective use in healthcare settings [5-8].

This paper seeks to comprehensively address the challenges posed by connected health devices, examining the potential impacts of these challenges and possible solutions to overcome them. The main contributions of our work are:

1) A detailed architectural overview of connected healthcare system, including their components and operational dynamics, is presented.

2) A thorough analysis of the vulnerabilities that render connected healthcare susceptible to security threats, scalability issues, storage limitations, and interoperability problems is conducted.

3) A comprehensive examination of the security challenges that arise when health devices are integrated into hospital networks, as well as an in-depth exploration of the issues that lead to scalability, storage, and interoperability problems, is provided.

4) A review of cutting-edge techniques and solutions aimed at addressing security, storage, scalability, and interoperability concerns in connected healthcare is presented.

5) Finally, this paper identifies and outlines several future research challenges, providing a roadmap for future researchers working in this rapidly evolving field.

The rest of the paper is structured as follows: In Section II, we provide a detailed insight into the architecture of the connected healthcare system. In Section III, we discuss the challenges faced by healthcare devices connected to the hospital network. In Section IV, we discuss the existing solutions used to address these challenges. Finally, in Section V, we explore possible future research challenges and conclude the paper.

II. CONNECTED HEALTHCARE SYSTEM

The concept of connected healthcare systems, which integrates various medical devices, such as patient monitoring systems, medical imaging devices, and wearable sensors, into the hospital network, has its roots in the early 2000s. This was when the healthcare industry began exploring ways to leverage technology, including EHRs telemedicine platforms, and health information exchanges (HIEs), to improve patient care and outcomes. Initially, this involved the adoption of HL7 (Health Level Seven) standards for data exchange, and later, the use of Fast Healthcare Interoperability Resources (FHIR) enabled more seamless data sharing between healthcare providers [9-13]. Over the years, the rapid growth of smartphones, wearables, and other digital devices has led to an explosion of health-related data, creating new opportunities for data-driven care, personalized medicine, and precision health [14-15]. The rise of cloud computing, artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) further enabled the integration of healthcare devices, systems, and services, giving rise to the modern connected healthcare system. Today, this system encompasses a vast network of interconnected devices, platforms, and stakeholders, working together to deliver more efficient, effective, and patient-centred care, leveraging technologies like edge computing, 5G networks, and block chain for secure and reliable data management [16-18].

A. Architecture of Connected Healthcare System

The Architecture of connected healthcare system is a multi-layered framework that enables the integration of various medical devices, systems, and services to facilitate data exchange, analysis, and decision-making across the healthcare ecosystem.

The device layer consists of various medical devices, sensors, and mobile devices that generate health-related data. This layer includes patient monitoring systems such as electrocardiogram (ECG) machines, blood pressure monitors, and pulse oximeters, which collect vital health data. Medical imaging devices like X-ray machines, computed tomography (CT) scanners, and magnetic resonance imaging (MRI) machines generate medical images. Sensors like temperature sensors, glucose sensors, and motion sensors collect additional health-related data. Mobile devices like smartphones and tablets, equipped with mobile apps, also collect data from patients. This layer is responsible for collecting, processing, and transmitting health-related data from patients to the Edge Layer for further analysis and processing. The devices in this layer use various communication protocols like Bluetooth, Wi-Fi, and cellular networks to transmit data, and utilize standards like HL7, FHIR, for data formatting and exchange [19-21].

When the transmitted medical data is received at the edge Layer, the edge layer processes and analyzes the data in real-time using gateways and edge servers. The gateways perform initial data processing, filtering, and aggregation, reducing the volume of information sent to the cloud or data center. Edge servers, built with edge computing frameworks like Azure Edge, AWS Edge, or Google Cloud Edge, enable faster processing, reduced latency, and improved real-time decision-making.

Furthermore, edge devices also perform basic analytics, such as trending and alerting, using machine learning algorithms to support timely interventions [22-24].

The important component of this architecture is the cloud layer which stores, processes, and analyzes data using cloud storage, computing, and services such as AI and ML. This layer provides scalable storage, computing resources, and advanced analytics capabilities, enabling the processing of large datasets and complex algorithms. Cloud-based services, such as AI and ML, support predictive analytics, pattern recognition, and personalized medicine [25-27].

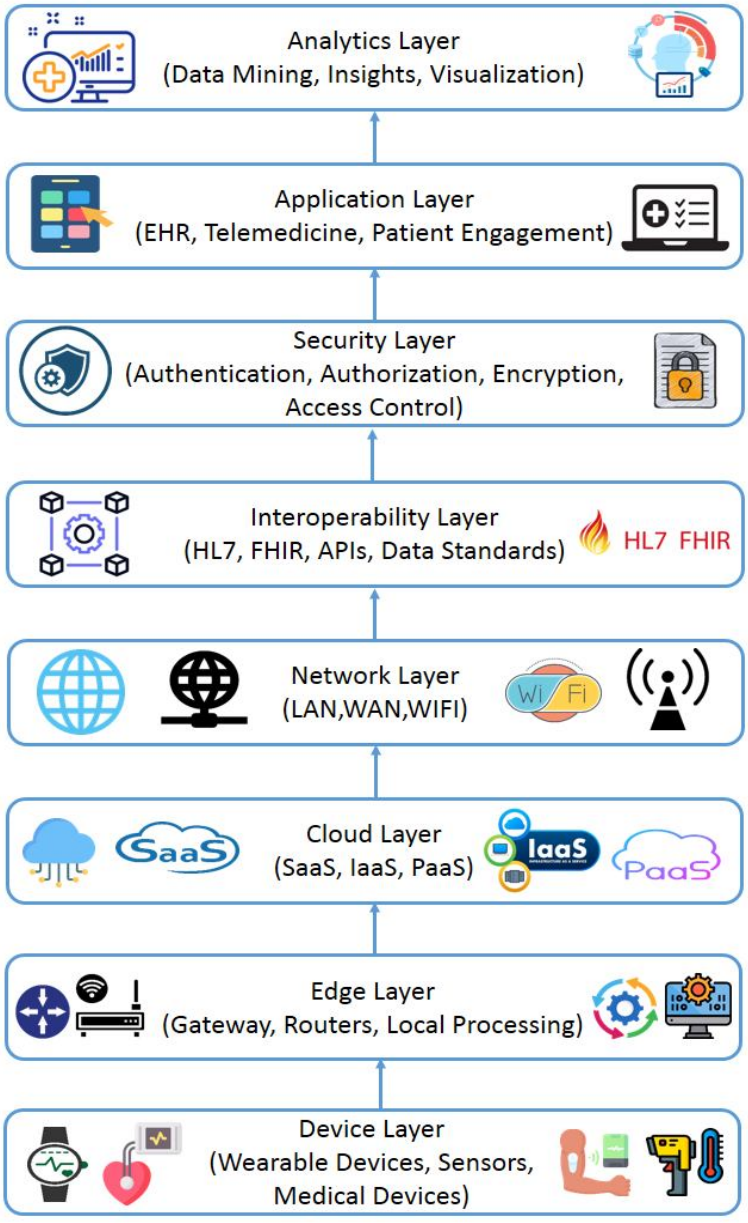


Figure 1 Connected healthcare System Architecture

The network layer is strong pillar of a connected healthcare system, providing seamless connectivity and data exchange between healthcare devices, systems, and services. It enables local and wide area networks, as well as internet connectivity, to facilitate communication and collaboration across different healthcare entities. By employing standardized network protocols like TCP/IP and HTTPS, the network layer ensures data integrity, confidentiality, and reliability during transmission. By supporting secure and reliable communication, this layers aims to play a vital role in delivering high-quality patient care, facilitating remote consultations, and enabling timely access to medical records and resources [28-31].

The connected healthcare system topmost layer is the application layer which provides a range of applications and services that support clinical decision-making, remote consultations, data analysis, and patient empowerment. This layer is utilized by various stakeholders, including healthcare professionals, patients, researchers, and healthcare organizations, to access data, conduct remote consultations, and make informed decisions. This layer consists of EHRs, telemedicine platforms, healthcare analytics tools, and patient engagement apps, which enable healthcare professionals to access patient data, conduct virtual consultations, and analyze data to inform treatment decisions. Patients can also use patient engagement apps to manage their health, access medical records, and communicate with healthcare providers [32-35].

The security layer is a critical component of connected healthcare, ensuring the confidentiality, integrity, and availability of patient data and medical information. To achieve this, the security layer employs robust security measures to protect against cyber threats, data breaches, and unauthorized access. These technical security measures include authentication protocols which verify user identities, as well as authorization techniques, like access control, which control access to sensitive data and systems. Furthermore, encryption protocols, like advanced encryption standard (AES) and Rivest-Shamir-Adleman (RSA), safeguard data both in transit and at rest. Additionally, firewalls, intrusion detection and prevention systems, and secure token services work together to restrict access to sensitive data and systems. Moreover, public key infrastructure and security information and event management systems manage digital certificates and monitor security-related data, ensuring the integrity of the security layer. All these measures work in concert to safeguard patient data and medical information, protecting against cyber threats and ensuring regulatory compliance [36-39]

The interoperability layer enables standards-based data exchange, application programming interfaces (APIs), and data transformation, facilitating the seamless sharing of data between different systems, services, and devices. This layer is crucial for supporting collaboration and coordinated care, as it enables healthcare providers, payers, and patients to access and share relevant information across organizational boundaries. Interoperability standards, such as HL7 and FHIR used here ensure seamless data exchange and integration, allowing healthcare organizations to share clinical data, claims data, and other relevant information. This layer data transformation capabilities ensure that data is converted into the required format, enabling seamless integration with various systems and applications. Through employment of these features, this layer plays a critical role in improving patient care while reducing the cost [40-42].

The final component of the connected healthcare system, is the analytics layer which performs data warehousing, mining, machine learning, predictive analytics, and business intelligence to support informed decision-making. This layer provides insights into patient outcomes, population health, and operational efficiency, enabling healthcare organizations to optimize resources, improve quality of care, and reduce cost. The layer utilizes cutting-edge technologies like Apache Hadoop, Amazon Redshift, SAS, R, Tableau, Power BI, TensorFlow, PyTorch, and natural language processing (NLP) to analyse structured and unstructured data, including data from wearable's, sensors, and other medical devices. By integrating these advanced analytics and AI capabilities, healthcare organizations drive innovation in healthcare delivery, and improve patient care [43-45].

III. CHALLENGES WITH MEDICAL DEVICES CONNECTED TO HOSPITAL NETWORK

The interaction of medical devices onto hospital network has induced a complex array of technical challenges, undermining the fundamental infrastructure of connected healthcare ecosystem. Specifically, the transmission of sensitive data over open communication channels has introduced vulnerabilities to cyber threats, necessitating robust security countermeasures [46]. Additionally, the integration of heterogeneous devices and systems has yielded interoperability complexities, while the exponential growth of connected devices has raised scalability concerns. Furthermore, the huge amount of generated data has created storage and management challenges, necessitating the need for data governance and analytics solutions [46]. In this section, we will explore in details the challenges faced by medical devices when connected with hospital network and what solution exists to overcome them.

A. Security Challenges

Security is a major concern in connected healthcare systems, as the sensitivity and critical nature of patient data make it an attractive target for cybercriminals. The open nature of communication between medical devices connected to hospital networks exposes them to various types of security attacks, potentially compromising patient care and endangering lives. For instance, an attacker can eavesdrop on communication, modify essential EHRs, and transmit altered information to hospital servers. Unaware of the modification, doctors may prescribe medication based on inaccurate data, putting patients at risk and compromising the effectiveness of the entire system.

The growth of advanced and smart medical devices connected to hospital networks has introduced a complex array of security challenges as shown in Figure 2, including:

1) *Authentication:* Verifying the identity of a user, device, or system to ensure they are who they claim to be [47].
2) *Integrity:* Preventing unauthorized modification or alteration of data [48].
3) *Confidentiality:* Ensuring that information is only shared with those who have a legitimate need to know, and that it is not accessed, read, or exploited by unauthorized individuals or systems [47].
4) *User Privacy:* Protection of personal information and data that identifies or relates to an individual user [48].
5) Availability: It refers to the assurance that a system, network, or data is accessible and usable when needed, without interruption or downtime [48].
6) *Forward Secrecy:* Ensuring that encrypted data remains protected even if encryption keys are compromised [47].
7) *Advanced Attacks:* Protecting against sophisticated threats such as:

a) Replay attacks: Intercepting and retransmitting data to manipulate systems [47].
b) Denial of Service (DoS) attacks: Overwhelming systems with traffic, rendering them unavailable [47].
c) Insider threats: Authorized personnel intentionally or unintentionally compromising security [47].
d) Modification attacks: Altering data or software to compromise system integrity [48].
e) Eavesdropping attacks: Intercepting sensitive data in transit [48].
f) Man-in-the-middle attacks: Intercepting and altering communication between devices and systems [48].

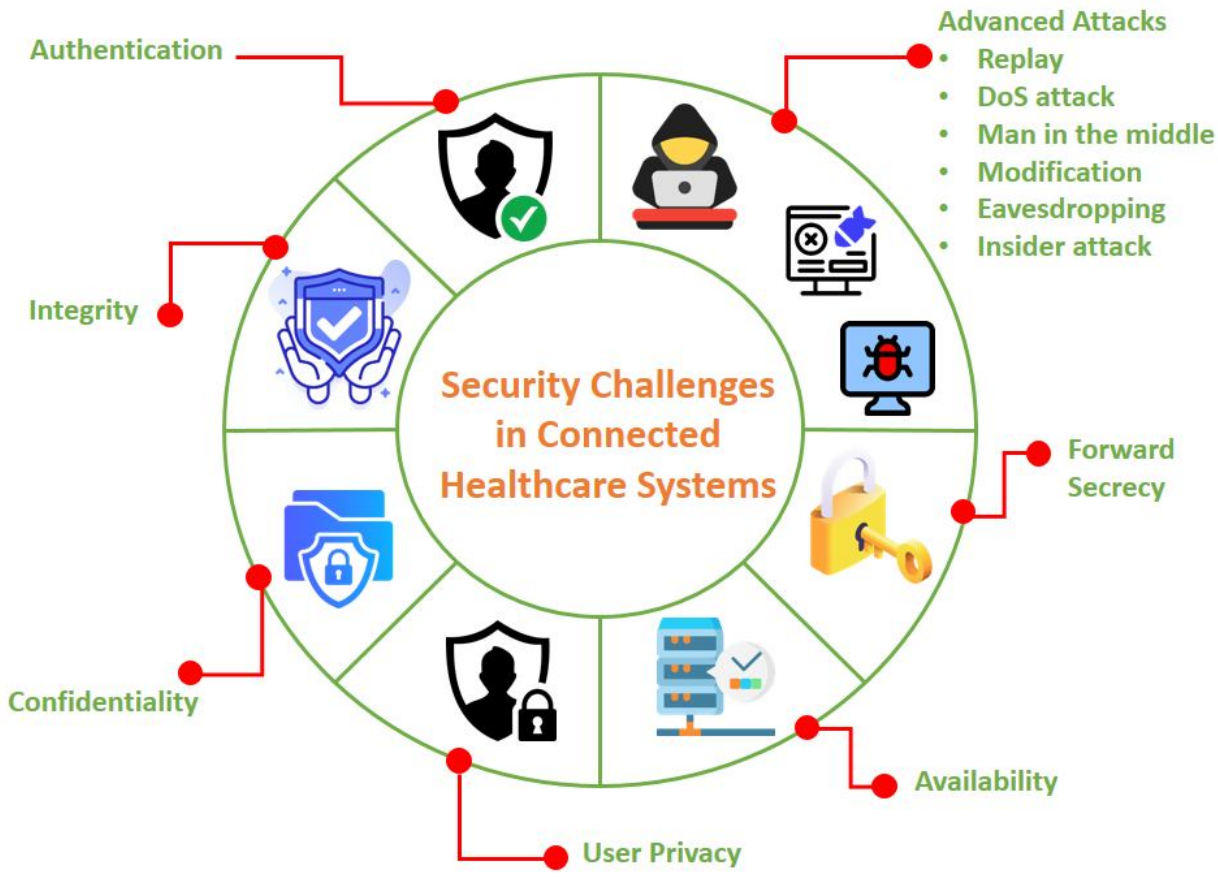


Figure 2 Security Challenges faced by medical devices connected to Healthcare Systems

Addressing these security challenges is crucial to ensuring the trustworthiness, reliability, and effectiveness of connected healthcare systems. Over the years, researchers have done considerable work to provide security for health systems in which medical devices are connected to hospital network.

Das et al., [49] designed mutual authentication mechanism for healthcare systems, utilizing lightweight cryptographic primitives such as XOR, concatenation, and hash operations. Their work enables secure sessions between authorized devices and gateways, preventing unauthorized access and ensuring device anonymity and un-traceability. Verma et al., [50] proposed an authentication and data aggregation mechanism for the Intelligent Healthcare System to address privacy, security, and data protection challenges. This protocol leverages Identity based cryptography and ensures robustness without pairing, offering provable security in the form of mutual authentication, privacy preservation and integrity. The author of [51] proposed a mechanism to secure the sensitive medical data stored in the cloud by leveraging advanced encryption techniques. They utilize an upgraded Advanced Encryption Standard (AES) for secure data storage and retrieval, and improved Elliptic Curve Cryptography (ECC) for key generation and validation. Their work successfully achieves integrity, confidentiality along with other security attributes. Alam et al., [52] proposed a protocol to enhance the security and efficiency of the Internet of Medical Things (IoMT) used for remote patient care during COVID-19. This protocol addresses issues of unauthorized access, ensuring both authentication and confidentiality while considering the constraints of IoMT devices, such as low energy and memory. The proposed solution is designed to protect patient information and improve healthcare delivery during pandemics. In [53] a key management mechanism was proposed for IoT-based healthcare, focusing on secure communication. Utilizing one-way accumulation and elliptic curve cryptography, the scheme ensures forward and backward secrecy by refreshing group keys as nodes join or leave. Their work effectively provide confidentiality, integrity and resistance against eavesdropping attack. Abutaleb et al., [54] put forward a blockchain-based framework for managing patient health records, ensuring that patients control access to their data. Utilizing hyper ledger Fabric and usage control (UCON), this system records all activities on an immutable ledger to enhance privacy and security. A new framework was proposed in [55] to enhance data encryption and authentication in internet of medical things. This technique combines optimal multi key homomorphic encryption and the improved social spider optimization algorithm for optimal key generation, aiming to ensure mutual authentication and reduce computational complexity while also offering confidentiality and resistance to eavesdropping and modification attacks. The authors of [56] proposed a security mechanism for smart health environments, aimed at remote monitoring scenarios. This technique employs multiple factors and a streamlined algorithm to address security vulnerabilities like impersonation attacks, replay attack and DoS attack and man in the middle attack. This approach not only improves operational efficiency but also ensures ease of use for healthcare professionals and patients, making it suitable for protecting patient privacy in the IoMT. In [57], an approach was designed to enhance the security of sensitive medical data within the IoMT ecosystem by using blockchain technology and smart contracts. This approach aims to create a decentralized, tamper-resistant platform that ensures data integrity, confidentiality, and controlled access. By integrating blockchain into IoMT, the proposed system address vulnerabilities and protect against data privacy breaches and cyber security threats. The authors of [58] designed a data aggregation scheme for the IoMT that ensures the anonymity of patients and fog nodes. This system uses authenticated servers for node registration and authentication, employing novel data aggregation and extraction algorithms. Their work offers security features in the form of user anonymity, insider attack resistance, replay attack resistance and man in the middle attack resistance.

These existing solutions demonstrates that addressing the security challenges in connected healthcare systems is crucial for protecting patient data and ensuring reliable healthcare delivery. The proposed solutions demonstrate significant advancements in providing authentication, encryption, and data management, along with resistance against known attacks while enhancing the security and privacy of medical information. Despite these existing solution, there is still room from improvement to provide robust and effective security with effective performance.

Table I Existing security solutions for connected healthcare

Security Challenge	Solution	Proposed Work	Features	Healthcare Domain
Authentication	Verifying user, device, or system identity	[49]	Mutual authentication, device anonymity, un-traceability	Connected Healthcare and Telemedicine
		[50]	Authentication, data aggregation, privacy preservation, integrity	Personalized Medicine
		[56]	Multi-factor authentication, streamlined algorithm, security for remote monitoring	Remote Patient Monitoring Application System

Integrity	Preventing unauthorized data modification	[51]	Advanced encryption (AES, ECC), secure data storage and retrieval	Medical Devices
		[53]	Key management, forward and backward secrecy, secure communication	Telemedicine Systems
Confidentiality	Ensuring data privacy and access control	[50]	Authentication, data aggregation, privacy preservation, integrity	Personalized Medicine
		[52]	Authentication, confidentiality, efficiency, remote patient care	Remote Patient Monitoring
User Privacy	Protecting personal information	[50]	Authentication, data aggregation, privacy preservation, integrity	Personalized Medicine
		[54]	Blockchain-based framework, patient-controlled access, immutable ledger	Electronic Health Records (EHRs)
Availability	Ensuring system and data accessibility	[52]	Authentication, confidentiality, efficiency, remote patient care	Remote Patient Monitoring
Forward Secrecy	Protecting encrypted data from compromised keys	[53]	Key management, forward and backward secrecy, secure communication	Telemedicine System
Advanced Attacks	Protecting against replay, DoS, insider, modification, eavesdropping, and man-in-the-middle attacks	[55]	Multi-key homomorphic encryption, optimal key generation, authentication	Healthcare Systems for Personalized Medicine
		[56]	Multi-factor authentication, streamlined algorithm, security for remote monitoring	Smart Healthcare System
		[57]	Decentralized blockchain technology and smart contracts.	Internet of Medical Things
		[58]	Data aggregation with privacy preservation	Internet of healthcare Things

B. Interoperability Challenges

Interoperability in connected healthcare is the ability of different systems, medical and health devices, and applications to communicate and exchange data seamlessly, enabling the sharing and use of information across different platforms and stakeholders. This is crucial for ensuring that patient data is accessible, shareable, and usable across different healthcare providers, payers, and patients themselves. Interoperability is necessary in connected healthcare to improve patient care, enhance efficiency, enable better decision-making, and empower patients [59-60]. However, achieving interoperability is fraught with challenges, including technical, semantic, organizational, security, privacy, scalability, legacy system, and regulatory barriers. Interoperability challenges in connected healthcare are multi face and complex and achieving Interoperability in connected healthcare systems is a difficult task to wide number of challenges. For instance technical challenges arise from different systems, devices, and applications using varying technical standards, protocols, and architectures, making integration and communication difficult. Semantic challenges occur when different systems and stakeholders interpret data differently, leading to inconsistencies and errors. Organizational challenges stem from different stakeholders having varying interests, priorities, and workflows, making collaboration and integration challenging. Security and privacy challenges require ensuring the security and privacy of patient data while facilitating interoperability. Scalability challenges require connected healthcare systems to accommodate the increasing amount of data and devices. Legacy system challenges involve integrating new systems with existing legacy systems, requiring significant resources and investment. Finally, regulatory challenges arise from regulatory requirements and laws, such as HIPAA, which can create barriers to interoperability [61-64]. Achieving interoperability in connected healthcare requires a unified approach to standards, protocols, and architectures. By bridging the gaps between systems, devices, and stakeholders, a seamless healthcare ecosystem is more than feasible. Researchers have performed numerous studies over the years and various solutions have been proposed to overcomes the barriers and achieve interoperability.

Guo et al., [65] suggested a novel information architecture to enhance semantic interoperability in healthcare systems, tackling the issue of ambiguous data interpretation across different platforms. By introducing an ostensive approach, they offer a complementary solution to existing lexical methods, showcasing its effectiveness through experiments with MIMIC III and diabetes datasets. This innovative Semantic Engine, built on an FHIR knowledge graph, facilitates semantic reasoning and patient-centric care. The authors of [66] proposes a decentralized access control model for secure interoperability in healthcare, enabling the safe exchange of data between organizations like hospitals, insurance companies, and pharmacies. This model utilizes ethereum blockchain technology to maintain a tamper-proof record of transactions and ensure authorized access to healthcare data. By implementing this model, healthcare organizations can collaborate and share data while maintaining security, transparency, and patient trust. The use of blockchain has been a driving factor for achieving interoperability. Jabbar et al., [67] introduced a blockchain-based framework for enhancing data interoperability and integrity in EHR sharing. Their work features an access management system for secure EHR exchange between medical providers and a decentralized Trusted Third Party Auditor (TTPA) ensuring data integrity. Pathak et al., [68] introduced scheme to achieve seamless device interoperability in IoT-based in-home healthcare monitoring systems, dubbed healthcare device interoperability. This system facilitates wireless connectivity among sensors, adapts to diverse sensor settings, and eliminates port dependencies, making it an ideal solution for scalable, portable, and user-friendly in-home health monitoring. In [69] a framework to address healthcare challenges by enhancing data interoperability among heterogeneous e-health system is proposed. Leveraging service-oriented architecture and web service technology, this approach enables seamless information exchange and integration. The resulting framework, guided by service-oriented analysis and design and supported by an interoperability matrix, serve as a reference for developing e-health systems in various healthcare applications. [70] proposed a framework for wearable healthcare devices, enabling seamless monitoring, decision-making, and control of sensor functionalities. Their framework adapts to the dynamic nature of various healthcare applications, optimizing device performance and interoperability. By accounting for device features and patient conditions, their approach facilitates autonomous and interconnected device operation, with adjustable frequency and time intervals for efficient tracking and improved healthcare outcomes.

Despite all these efforts by researchers, the majority of healthcare data exchange is limited to syntactic interoperability, where data is exchanged in a standardized format, but the meaning and context of the data are not fully understood. To achieve true semantic interoperability, where data is not only exchanged but also accurately interpreted and utilized, additional work is required to address the complexities of data context, terminology, and logic. Furthermore, the development of advanced data analytics and artificial intelligence capabilities, as well as the integration of IoT devices and wearables, will require continued evolution and refinement of interoperability standards to ensure seamless data exchange and optimal patient care.

Table II Interoperability Challenges in Connected Healthcare

Challenge	Description	Impact on Connected Healthcare
Data Standards	Lack of common data standards and formats	Delays in remote patient monitoring, inaccurate telemedicine diagnoses
Semantic Interoperability	Difficulty in achieving shared understanding of data meaning and context	Ineffective personalized medicine, poor population health management
Security and Privacy	Ensuring secure data exchange and protecting patient privacy	Cyberattacks on connected healthcare platforms, compromised patient data
Device and System Integration	Integrating diverse devices, systems, and applications	Incompatible wearables and mobile apps, disrupted continuous care
Scalability and Flexibility	Accommodating growing data volumes and evolving healthcare needs	Overwhelmed connected healthcare infrastructure, inability to handle surge in remote consultations
Data Quality and Validation	Ensuring accuracy, completeness, and reliability of exchanged data	Inaccurate remote patient monitoring data, poor clinical decision-making
Regulatory and Standards Compliance	Meeting diverse regulatory and standards requirements	Non-compliance with HIPAA, GDPR, and other regulations, legal issues
Sustainability and Maintenance	Ensuring long-term sustainability and maintenance of interoperability solutions	Discontinued support for connected healthcare platforms, data exchange disruptions

1) Level-1 Interoperability Standards

In the connected healthcare domain, interoperability standards facilitate the syntactic and semantic matching of data, enabling the effective communication and exchange of clinical and administrative information between heterogeneous systems. Globally, a range of interoperability standards have been developed and implemented to address the complexities of healthcare data exchange, including:

- Health Level Seven (HL7): A set of international standards for exchanging clinical and administrative data between healthcare applications, enabling the sharing of patient information, laboratory results, and medical billing [71].
- Fast Healthcare Interoperability Resources (FHIR): A standard for exchanging healthcare information electronically, using APIs and data formats, facilitating secure and efficient data sharing between healthcare providers, payers, and patients [72].
- Digital Imaging and Communications in Medicine (DICOM): A standard for medical imaging data exchange, enabling the sharing and interpretation of medical images, such as X-rays and MRIs, between healthcare providers and facilities [73].
- SNOMED-CT (Systematized Nomenclature of Medicine - Clinical Terms): A comprehensive clinical terminology standard for EHRs, enabling accurate and consistent coding and classification of clinical data [74].
- ICD-10 (International Classification of Diseases, 10th Revision): A standard for coding and classification of diseases, injuries, and causes of death, facilitating accurate data exchange and analysis [75].
- ISO/IEEE 11073 (Medical Device Communication Standards): A set of standards for medical device communication, enabling the secure and efficient exchange of data between medical devices, such as patient monitors and ventilators [76].

These interoperability standards enable healthcare providers, payers, and patients to access and share information securely, efficiently, and accurately, regardless of the technology or platform used, ultimately improving patient care and outcomes. By adopting these standards, healthcare organizations can ensure seamless data exchange, reduce errors, and enhance the overall quality of care. Additionally, these standards facilitate the sharing of best practices, research, and innovation, contributing to the advancement of healthcare globally.

C. Scalability Challenges

The increasing number of healthcare devices connected to hospitals poses significant scalability challenges. The amount of data produced increases along with the number of devices, posing challenges in data management, storage, and analysis. Additionally, the diversity of devices, protocols, and data formats creates complexity in integrating and interoperating with existing hospital systems [77-78]. Connected healthcare systems face scalability issues when they are unable to handle increased traffic, data volume, and user demand without compromising performance, reliability, and security. This occurs when the system's resources, such as processing power, memory, and storage are unable to accommodate the increasing number of connected devices, users, and data transactions [78-79]. Such scalability issues can have a drastic impact on connected heath care system such as

1) If system is down, resulting in delayed or lost critical patient data, disrupted clinical workflows, and compromised patient care.
2) Inadequate storage and processing capabilities can lead to data loss, corruption, or inconsistencies, compromising patient safety and care quality.
3) Scalability issues create vulnerabilities that cybercriminals can exploit, compromising patient data privacy and security.
4) Slow system response times delay critical decision-making, affecting patient outcomes and care quality.
5) Poor system performance and reliability discourage healthcare professionals from adopting connected healthcare solutions, hindering efficient care delivery.

To overcome these scalability issues, researchers over the years have proposed several solutions. Yang et al., [80] proposed service-oriented architecture based healthcare information system, which prioritize scalability in both hardware and software. Their work integrates heterogeneous systems through a standardized HL7 service interface, enabling scalable and efficient exchange of healthcare data across various applications and devices. The authors of [81] introduced an e-health monitoring architecture that leverages sensors, cloud, and fog infrastructure to provide real-time patient care and multimedia health services. To ensure system reliability, the author also proposes stochastic models examine how failures affect the availability of the system. The proposed architecture and models aim to identify and mitigate potential failures, particularly in emergency scenarios, to ensure optimal patient outcomes. [82] worked to handle high latency issues, and put forward a solution, combining an analytical model and a hybrid fuzzy-based reinforcement learning algorithm in a fog computing environment. This approach reduces latency among healthcare IoT, end-users, and cloud servers. In [83] a work is produced which leverages blockchain technology to enhance the privacy, security, and scalability of healthcare data in IoMT platforms.

The approach utilizes smart contracts to ensure secure and decentralized storage and communication of patient data, addressing concerns of centralized IoMT structures. This framework aims to revolutionize healthcare data management, ensuring confidentiality, integrity, and availability of patient information along with effectively providing scalability. The authors of [84] propose an architecture for smart healthcare, which combines blockchain and federated learning to protect user data privacy and preventing data loss. This approach utilizes blockchain-driven Internet of Things cloud systems enabling federated learning and security in large-scale machine learning applications. In smart city healthcare, users can acquire a well-trained machine learning model without disclosing personal information, guaranteeing security and privacy.

Table III Proposed Solutions for Scalability Issues in Connected Healthcare

Reference	Solution	Key Features	Benefits
[80]	Service-oriented architecture	Scalable hardware and software, HL7 service interface	Efficient data exchange, scalability
[81]	Edge, fog and cloud infrastructure with stochastic models	Sensors, cloud, fog infrastructure, stochastic models	Real-time patient care, system reliability, optimal patient outcomes
[82]	Hybrid fuzzy-based reinforcement learning	Analytical model, fog computing environment	Reduced latency, improved IoT data transmission
[83]	Blockchain	Smart contracts, decentralized storage and communication	Enhanced privacy, security, scalability, confidentiality, integrity, and availability
[84]	Blockchain and federated learning architecture	Blockchain-based IoT cloud platforms, federated learning	Protected user data privacy, prevented data loss, scalable machine learning

D. Storage Concerns

The rapid growth of healthcare data, fueled by the increasing number of connected devices and systems, poses significant storage challenges. Healthcare data storage solutions come in three forms: onsite, cloud, and hybrid. Onsite storage solutions are typically used for sensitive data that requires high security and low latency, while cloud storage solutions offer scalability and cost-effectiveness. Hybrid storage solutions combine the benefits of both, but can be complex to manage. However, these solutions can be inefficient when working with substantial amounts of data, diverse data formats, and real-time data generation. For instance, onsite storage can be costly and limited in capacity, while cloud storage may raise security and compliance concern and lastly, hybrid storage can be challenging to manage and integrate [85-88].

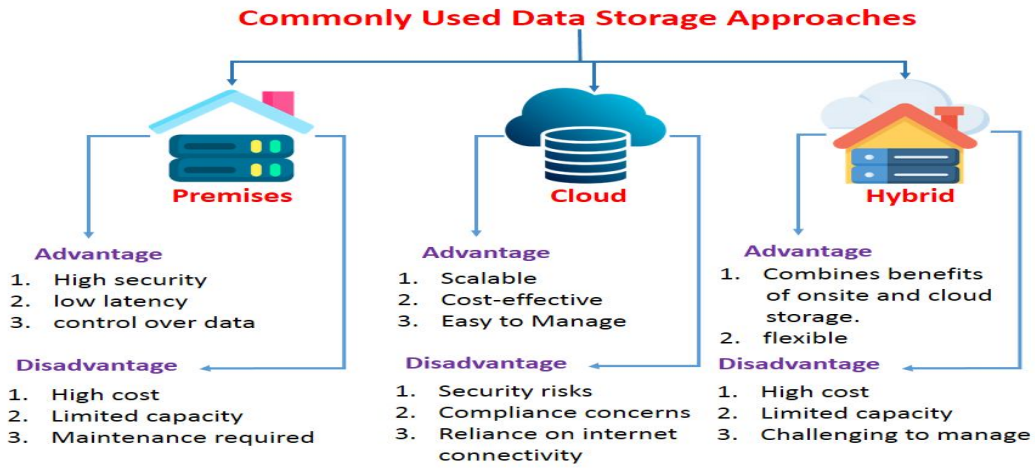


Figure 3 Commonly used data storage approaches in connected healthcare

The data deluge from medical imaging machines, patient monitoring systems, and EHRs can quickly overwhelm storage capacities, and the diverse range of devices and systems produce data in various formats, making management and storage challenging. Real-time data generation from devices such as patient monitoring systems requires high-speed storage solutions to keep pace with the data influx, and ensuring the accuracy, completeness, and integrity of healthcare data is crucial, but difficult, particularly when handling big data sets. If not addressed, these storage challenges can lead to data loss, system downtime, security risks, inefficient data management, and compliance violations, ultimately impacting patient care and outcomes [89-90].

Researchers have been actively exploring innovative solutions to address these storage-related challenges, and several recent studies have proposed effective strategies to mitigate these issues. The work by Firouzi et al., [91] put forward a solution in the form of data monetization strategy that leverages the potential of IoT data, enabling organizations to capitalize on their data assets through data-driven decision making, data-enriched product and service offerings, and data marketplaces. They also put up an approach for the architecture of the healthcare data economy that tackled important issues including security, scalability, and data governance. The author also explores the application of privacy-preserving technologies like multiparty computation and machine learning to ensure the secure and ethical use of healthcare data. In [92], a federated learning framework to address the storage challenges of healthcare data fragmentation, enabling the aggregation of decentralized data from various sources, such as electronic EHRs, without compromising data privacy. This approach facilitates the training of a shared global model on distributed data, leveraging a central server to orchestrate the learning process while maintaining data locality and confidentiality. Blockchain has been a state of the art technology for handling these storage challenges in connected healthcare. In [93], a work is proposed which is based on blockchain-based for handling storage issues of personal medical data, leveraging decentralization, verifiability, and immutability to ensure secure and efficient storage and sharing. This approach utilizes a combination of blockchain and cloud storage to manage medical records, eliminating reliance on third-party intermediaries and preventing any single entity from controlling the data. The proposed framework enables secure, decentralized, and patient-centric management of medical information. The article [94] explores the potential of blockchain technology to transform HER systems, addressing issues of data security and storage, integrity, and management. A framework is proposed for implementing blockchain in healthcare, ensuring secure storage and granular access control for EHRs, while also addressing scalability concerns through off-chain storage. The framework aims to provide a scalable, secure, and integral blockchain-based solution for EHR systems, revolutionizing healthcare data management.

IV. THE WAY AHEAD: TACKLING CHALLENGES AND SEIZING OPPORTUNITIES

As the healthcare industry continues to cope with the challenges of medical devices when connected to hospital network, it is essential to prioritize strategies that address these issues head-on. In this section, we outline future research directions and key recommendations for stakeholders to tackle these challenges.

The security of connected healthcare systems is a top priority for any healthcare organization. Developing robust encryption and authentication protocols is essential to protect sensitive data and prevent unauthorized access. While current research has focused intensively on this aspect, existing solutions fall short due to their reliance on resource-intensive cryptographic algorithms that require significant processing power and storage capabilities. However, medical devices, sensors, and other wearable devices have limited resources, making it crucial to develop lightweight cryptographic mechanisms that achieve robust security without compromising performance. Researchers have suggested ways to improve interoperability, but current solutions are limited by proprietary protocols and data formats, creating a fragmented system that leads to communication problems, data silos, and errors, making it hard to share patient information smoothly. Subsequent work must concentrate on establishing more standardized communication protocols and APIs to facilitate effortless data sharing, ensure accuracy, and enable real-time insights. Standardization may facilitate a more cohesive and efficient healthcare system, enabling better patient care and improved outcomes.

Current scalability solutions for connected healthcare fall short due to limited infrastructure and rigid device designs, hindering the ability in order to manage growing data volumes and device connections. To meet the growing demands of connected healthcare, it's essential to scale for the future. This can be achieved by leveraging cloud-based solutions for data storage and processing, allowing for greater flexibility and scalability. Additionally, implementing artificial intelligence and machine learning for predictive maintenance enables proactive device management and minimizes downtime. Furthermore, developing modular and adaptable device designs enables easy integration and upgrade, ensuring a future-proof connected healthcare ecosystem.

Existing storage solutions for connected healthcare are struggling to keep up with the vast volumes of data being produced, leading to data silos, fragmentation, and increased costs. Current storage systems are often inefficient, inflexible, and vulnerable to data corruption and loss. In future, the solutions must prioritize data consolidation, redundancy, and backup, leveraging technologies like cloud storage, data archiving, and disaster recovery to ensure reliable and secure data storage.

Researchers have progressed well in the domain of data analytics since the advancement of machine learning however, existing data analytics in healthcare is limited by fragmented data, delayed insights, poor data quality, and lack of interoperability, limited contextual understanding. In future, researchers should focus on developing advanced data analytics tools for real-time monitoring and insights enables healthcare professionals to make informed decisions quickly. Integrating data from multiple devices and sources provides a thorough understanding of patients' health. Using data-driven approaches for quality improvement and patient safety leads to better health outcomes.

Lastly, and most importantly it is necessary to establish clear guidelines for device connectivity and data management ensures a secure and efficient connected healthcare ecosystem. Encouraging collaboration between industry stakeholders and regulatory bodies facilitates the development of effective regulations. Developing standards for device security and interoperability promotes trust and confidence in connected healthcare technologies.

V. CONCLUSIONS

The rapid digital transformation in healthcare has increased a profound reliance on medical devices and sensors, revolutionizing healthcare delivery through advanced patient monitoring, remote care, and data-driven decision-making. This connected healthcare paradigm has yielded significant improvements in patient outcomes and healthcare efficiency. However, the integration of medical devices into hospital networks also raises critical concerns about security, scalability, storage, and interoperability, increasing the risk of cyber-attacks, data breaches, and system downtime. As the healthcare ecosystem increasingly relies on connected devices, addressing these challenges is crucial to ensure continued patient care improvement and sensitive medical data protection. This paper provides a comprehensive examination of connected healthcare challenges ranging from authentication challenges, confidentiality issues to more advanced security threats such as man in the middle attack, replay attack and others, scalability limitations, storage constraints, and interoperability issues that arise when medical devices are integrated into hospital networks. We also thoroughly explore existing solutions proposed to address these challenges but majority of proposed solutions aren't built while keeping in mind the resource constraint nature of sensors, medical devices which make it difficult for these devices to perform heavy processing to store huge data. We also expressed other limitations of existing solution highlighting the need for future research and indicated key areas for future research. Furthermore, we examine the role of emerging technologies, such as AI and blockchain, in addressing the challenges of connected healthcare. By recognizing these issues and suggesting potential solutions, we hope to support the development of more secure, scalable, and interoperable connected healthcare systems.

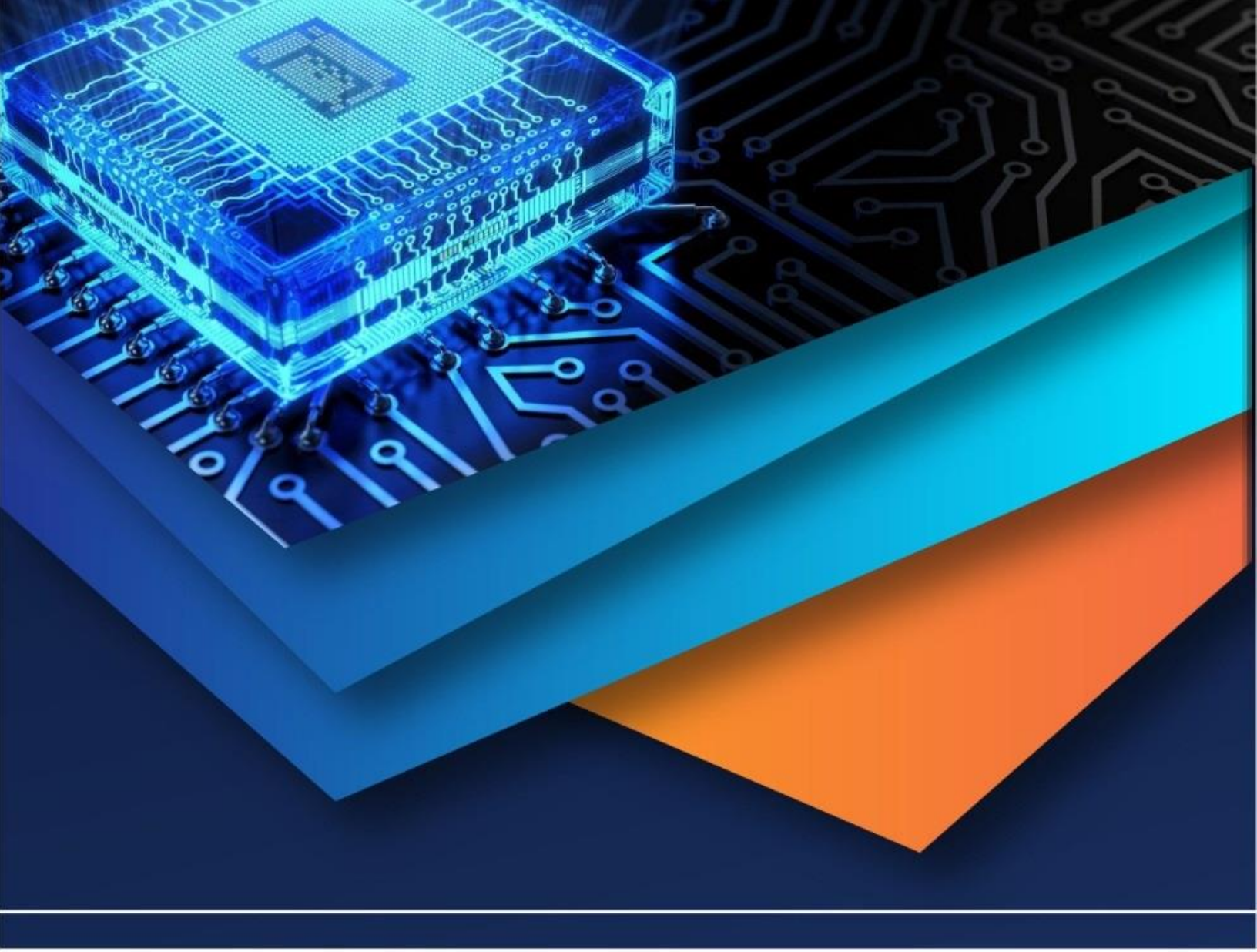
REFERENCES

[1] Osama M, Ateya AA, Sayed MS, Hammad M, Pławiak P, Abd El-Latif AA, Elsayed RA. Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. Sensors. 2023 Aug 25;23(17):7435. doi: 10.3390/s23177435.
[2] Ahmed SF, Alam MSB, Afrin S, Rafa SJ, Rafa N, Gandomi AH. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion [Internet]. 2023;102060.doi: /10.1016/j.inffus.2023.102060
[3] Rani S, Kumar S, Kataria A, Min H. SmartHealth: An intelligent framework to secure IoMT service applications using machine learning. ICT Express. 2024 Apr 1;10(2):425-30. doi: 10.1016/j.icte.2023.10.001
[4] Telemedicine Market Analysis, 2026 | Size, Share, Growth, Research [Internet]. www.fortunebusinessinsights.com. Available from: https://www.fortunebusinessinsights.com/industry-reports/telemedicine-market-101067.
[5] Abounassar EM, El-Kafrawy P, Abd El-Latif AA. Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey. Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions. 2022:159-89. doi: 10.1007/978-3-030-85428-7_7.
[6] Karatas M, Eriskin L, Deveci M, Pamucar D, Garg H. Big Data for Healthcare Industry 4.0: Applications, challenges and future perspectives. Expert Systems with Applications. 2022 Aug 15;200:116912. doi: 10.1016/j.eswa.2022.116912
[7] Selvaraj S, Sundaravaradhan S. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences. 2020 Jan;2(1):139. doi: 10.1007/s42452-019-1925-y.
[8] Somasundaram R, Thirugnanam M. Review of security challenges in healthcare internet of things. Wireless Networks. 2021 Nov;27(8):5503-9. doi: 10.1007/s11276-020-02340-0.
[9] Serbanati LD. Health digital state and Smart EHR systems. Informatics in Medicine Unlocked. 2020 Jan 1;21:100494. doi: 10.1016/j.imu.2020.100494.
[10] Gupta S, Sharma HK, Kapoor M. Smart Healthcare and Telemedicine Systems: Present and Future Applications. Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). 2022 Dec 15; 183–197. doi: 10.1007/978-3-031-18896-1_15.
[11] Mutanu L, Gupta K, Gohil J. Leveraging IoT solutions for enhanced health information exchange. Technology in Society. 2022 Feb 1;68:101882. doi: 10.1016/j.techsoc.2022.101882.
[12] Joyia GJ, Akram MU, Akbar CN, Maqsood MF. Evolution of health level-7: A survey. In Proceedings of the 2018 International Conference on Software Engineering and Information Management. 2018 Jan 4; 118-123. doi: 10.1145/3178461.3178480.
[13] Amar F, April A, Abran A. Electronic Health Record and Semantic Issues Using Fast Healthcare Interoperability Resources: Systematic Mapping Review. Journal of medical Internet research. 2024 Jan 30;26:e45209. doi:10.2196/45209.
[14] Formica D, Schena E. Smart sensors for healthcare and medical applications. Sensors. 2021 Jan 14;21(2):543. doi: 10.3390/s21020543.

[15] Gardašević G, Katzis K, Bajić D, Berbakov L. Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. Sensors. 2020 Jun 27;20(13):3619. doi: 10.3390/s20133619.
[16] Alnaim AK, Alwakeel AM. Machine-learning-based IoT–edge computing healthcare solutions. Electronics. 2023 Feb 18;12(4):1027. doi: 10.3390/electronics12041027.
[17] Omrčen L, Leventić H, Romić K, Galić I. Integration of Blockchain and AI in EHR sharing: A survey. In 2021 International Symposium ELMAR 2021 Sep 13; 155-160. IEEE. doi: 10.1109/ELMAR52657.2021.9550953.
[18] Sharma A, Singh M, Gupta M, Sukhija N, Aggarwal PK. IoT and blockchain technology in 5G smart healthcare. In Blockchain Applications for Healthcare Informatics 2022 Jan 1; 137-161. doi: B978-0-323-90615-9.00004-9.
[19] Wu F, Wu T, Yuce MR. An internet-of-things (IoT) network system for connected safety and health monitoring applications. Sensors. 2018 Dec 21;19(1):21. doi: 10.3390/s19010021.
[20] Loncar-Turukalo T, Zdravevski E, Machado da Silva J, Chouvarda I, Trajkovik V. Literature on Wearable Technology for Connected Health: Scoping Review of Research Trends, Advances, and Barriers. Journal of Medical Internet Research. 2019 Sep 5;21(9):e14017. doi: 10.2196/14017.
[21] Rana A, Chakraborty C, Sharma S, Dhawan S, Pani SK, Ashraf I. Internet of Medical Things-Based Secure and Energy-Efficient Framework for Health Care. Big Data. 2021 Dec 24; doi: 10.1089/big.2021.0202
[22] Ben Dhaou I, Ebrahimi M, Ben Ammar M, Bouattour G, Kanoun O. Edge devices for internet of medical things: technologies, techniques, and implementation. Electronics. 2021 Aug 31;10(17):2104. doi: 10.3390/electronics10172104.
[23] Parah SA, Kaw JA, Bellavista P, Loan NA, Bhat GM, Muhammad K, de Albuquerque VH. Efficient security and authentication for edge-based internet of medical things. IEEE Internet of Things Journal. 2020 Nov 13;8(21):15652-62. doi: 10.1109/JIOT.2020.3038009.
[24] Awad AI, Fouda MM, Khashaba MM, Mohamed ER, Hosny KM. Utilization of mobile edge computing on the Internet of Medical Things: A survey. ICT Express. 2022 May 19. doi: 10.1016/j.icte.2022.05.006.
[25] Tahir S, Bakhsh ST, Abulkhair M, Alassafi MO. An energy-efficient fog-to-cloud Internet of Medical Things architecture. International Journal of Distributed Sensor Networks. 2019 May;15(5):1550147719851977. doi: 10.1177/1550147719851977.
[26] Sun L, Jiang X, Ren H, Guo Y. Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. IEEE access. 2020 May 26;8:101079-92. doi: 10.1109/ACCESS.2020.2997831.
[27] Cao R, Tang Z, Liu C, Veeravalli B. A scalable multicloud storage architecture for cloud-supported medical internet of things. IEEE Internet of Things Journal. 2019 Oct 8;7(3):1641-54. doi: 10.1109/JIOT.2019.2946296.
[28] Naresh VS, Pericherla SS, Murty PS, Reddi S. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions. Computer Systems Science & Engineering. 2020 Nov 1;35(6). doi: 10.32604/csse.2020.35.411.
[29] Dey N, Ashour AS, Bhatt C. Internet of things driven connected healthcare. Internet of things and big data technologies for next generation healthcare. 2017:3-12. doi:10.1007/978-3-319-49736-5_1.
[30] Wei K, Zhang L, Guo Y, Jiang X. Health monitoring based on internet of medical things: architecture, enabling technologies, and applications. IEEE Access. 2020 Feb 4;8:27468-78. doi: 10.1109/ACCESS.2020.2971654.
[31] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet of Things Journal. 2020 Dec 17;8(11):8707-18. doi: 10.1109/JIOT.2020.3045653.
[32] Bansal M, Priya. Application Layer Protocols for Internet of Healthcare Things (IoHT). 2020 Fourth International Conference on Inventive Systems and Control (ICISC). 2020 Jan 1. doi: 10.1109/ICISC47916.2020.9171092
[33] Safaei B, Monazzah AM, Bafroei MB, Ejlali A. Reliability side-effects in Internet of Things application layer protocols. In 2017 2nd International Conference on System Reliability and Safety (ICSRS) 2017 Dec 20; 207-21. doi: 10.1109/ICSRS.2017.8272822.
[34] Abbasi M, Plaza-Hernández M, Prieto J, Corchado JM. Security in the internet of things application layer: requirements, threats, and solutions. IEEE Access. 2022 Sep 8;10:97197-216. doi: 10.1109/ACCESS.2022.3205351.
[35] Balasubramanian V, Jolfaei A. A scalable framework for healthcare monitoring application using the Internet of Medical Things. Software: Practice and Experience. 2021 Dec;51(12):2457-68. doi: 10.1002/spe.2849.
[36] Sun Y, Lo FP, Lo B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access. 2019 Dec 18;7:183339-55. doi: 10.1109/ACCESS.2019.2960617.
[37] Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis C. Review of security and privacy for the Internet of Medical Things (IoMT). In2 019 15th international conference on distributed computing in sensor systems (DCOSS) 2019 May 29: 457-464. doi: 10.1109/DCOSS.2019.00091.
[38] Behrens R, Ahmed A. Internet of Things: An end-to-end security layer. In2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN) 2017 Mar 7: 146-149. doi: 10.1109/ICIN.2017.7899405.
[39] Singh D, Tripathi G, Jara A. Secure layers based architecture for Internet of Things. In2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) 2015 Dec 14 : 321-326. doi: 10.1109/WF-IoT.2015.7389074.
[40] Rubí JN, Gondim PR. Interoperable internet of medical things platform for e-health applications. International Journal of Distributed Sensor Networks. 2020 Jan; 16(1):1550147719889591.doi: 10.1177/1550147719889591.
[41] Abounassar EM, El-Kafrawy P, Abd El-Latif AA. Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey. Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions. 2022:159-89. doi: 10.1007/978-3-030-85428-7_7.
[42] Jaleel A, Mahmood T, Hassan MA, Bano G, Khurshid SK. Towards medical data interoperability through collaboration of healthcare devices. IEEE Access. 2020 Jul 16; 8:132302-19. doi: 10.1109/ACCESS.2020.3009783.
[43] Rehman A, Haseeb K, Saba T, Lloret J, Tariq U. Secured big data analytics for decision-oriented medical system using internet of things. Electronics. 2021 May 27; 10(11):1273. doi: 10.3390/electronics10111273.
[44] Manogaran G, Lopez D, Thota C, Abbas KM, Pyne S, Sundarasekar R. Big data analytics in healthcare Internet of Things. Innovative healthcare systems for the 21st century. 2017:263-84. doi: 10.1007/978-3-319-55774-8_10.
[45] Plageras AP, Stergiou C, Kokkonis G, Psannis KE, Ishibashi Y, Kim BG, Gupta BB. Efficient large-scale medical data (ehealth big data) analytics in internet of things. In2017 IEEE 19th Conference on Business informatics (CBI) 2017 Jul 24: 21-27. doi: 10.1109/CBI.2017.3.

[46] Sharmila EM, Rama Krishna K, Prasad GN, Anand B, Kwatra CV, Kapila D. IoMT—Applications, Benefits, and Future Challenges in the Healthcare Domain. Advances in Fuzzy-Based Internet of Medical Things (IoMT). 2024 Jun 28:1-23. doi: 10.1002/9781394242252.ch1
[47] Bhushan B, Kumar A, Agarwal AK, Kumar A, Bhattacharya P, Kumar A. Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. Sustainability. 2023 Apr 3; 15(7):6177. doi: 10.3390/su15076177.
[48] Wani RU, Thabit F, Can O. Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review. Security and Privacy. 2023 Apr 19:e409. doi: 10.1002/spy2.409.
[49] Das S, Namasudra S. Lightweight and efficient privacy-preserving mutual authentication scheme to secure Internet of Things-based smart healthcare. Transactions on Emerging Telecommunications Technologies. 2023 Nov; 34(11):e4716. doi: 10.1002/ett.4716.
[50] Verma P, Gupta DS. A pairing-free data authentication and aggregation mechanism for intelligent healthcare system. Computer Communications. 2023 Jan 15: 198:282-96. doi: 10.1016/j.comcom.2022.12.009.
[51] Patnaik A, Krishna Prasad K. Secure Authentication and Data Transmission for Patients Healthcare Data in Internet of Medical Things. International journal of mathematical, engineering and management sciences. 2023 Oct 1; 8(5):1006–23. doi: 10.33889/IJMEMS.2023.8.5.058.
[52] Alam I, Kumar M. A novel authentication protocol to ensure confidentiality among the Internet of Medical Things in covid-19 and future pandemic scenario. Internet of Things. 2023 Jul 1; 22:100797. doi: 10.1016/j.iot.2023.100797.
[53] Trivedi C, Rao UP. Secrecy aware key management scheme for Internet of Healthcare Things. The Journal of Supercomputing. 2023 Jul; 79(11):12492-522. doi: 10.1007/s11227-023-05144-z.
[54] Abutaleb RA, Alqahtany SS, Syed TA. Integrity and privacy-aware, patient-centric health record access control framework using a blockchain. Applied Sciences. 2023 Jan 12; 13(2):1028. doi: 10.3390/app13021028.
[55] Riya KS, R. Surendran, Andr C, M. Sadish Sendil. Encryption with User Authentication Model for Internet of Medical Things Environment. Intelligent Automation and Soft Computing. 2023 Jan 1;35(1):507–20. doi:10.32604/iasc.2023.027779.
[56] Ali Z, Mahmood S, Mansoor K, Daud A, Alharbey R, Bukhari A. A Lightweight and Secure Authentication Scheme for Remote Monitoring Of Patients in IOMT. IEEE Access. 2024 May 13. doi: 10.1109/ACCESS.2024.3400400.
[57] Chatterjee P, Das D, Banerjee S, Ghosh U, Mpembele AB, Rogers T. An Approach towards the Security Management for Sensitive Medical Data in the IoMT Ecosystem. In Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing 2023 Oct 23: 400-405 .doi: 10.1145/3565287.3623388.
[58] Chakraborty C, Othman SB, Almalki FA, Sakli H. FC-SEEDA: Fog computing-based secure and energy efficient data aggregation scheme for Internet of healthcare Things. Neural Computing and Applications. 2024 Jan;36(1):241-57. doi: 10.1007/s00521-023-08270-0
[59] Vorisek CN, Lehne M, Klopfenstein SA, Mayer PJ, Bartschke A, Haese T, Thun S. Fast healthcare interoperability resources (FHIR) for interoperability in health research: systematic review. JMIR medical informatics. 2022 Jul 19;10(7):e35724. doi:10.2196/35724.
[60] de Mello BH, Rigo SJ, da Costa CA, da Rosa Righi R, Donida B, Bez MR, Schunke LC. Semantic interoperability in health records standards: a systematic literature review. Health and technology. 2022 Mar;12(2):255-72. doi: 10.1007/s12553-022-00639-w.
[61] Reegu F, Daud SM, Alam S. Interoperability challenges in healthcare blockchain system-a systematic review. Annals of the Romanian Society for Cell Biology. 2021 May 12:15487-99.
[62] Ndlovu K, Scott RE, Mars M. Interoperability opportunities and challenges in linking mhealth applications and eRecord systems: Botswana as an exemplar. BMC medical informatics and decision making. 2021 Aug 21; 21(1):246. doi:10.1186/s12911-021-01606-7
[63] Albouq SS, Abi Sen AA, Almashf N, Yamin M, Alshanqiti A, Bahbouh NM. A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access. 2022 Mar 25; 10: 36416-28. doi: 10.1109/ACCESS.2022.3162219 .
[64] Lee E, Seo YD, Oh SR, Kim YG. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials. 2021 Mar 19;23(2):1020-47. doi: 10.1109/COMST.2021.3067354.
[65] Guo H, Scriney M, Liu K. An ostensive information architecture to enhance semantic interoperability for healthcare information systems. Information Systems Frontiers. 2024 Feb; 26(1):277-300. doi: 10.1007/s10796-023-10379-5.
[66] Rana SK, Rana SK, Nisar K, Ag Ibrahim AA, Rana AK, Goyal N, Chawla P. Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare. Sustainability. 2022 Aug 2;14(15):9471. doi: 10.3390/su14159471.
[67] Jabbar R, Fetais N, Krichen M, Barkaoui K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) 2020 Feb 2: 310-317. doi: 10.1109/ICIoT48696.2020.9089570.
[68] Pathak N, Misra S, Mukherjee A, Kumar N. HeDI: Healthcare device interoperability for IoT-based e-health platforms. IEEE Internet of Things Journal. 2021 Jan 18;8(23):16845-52. doi:: 10.1109/JIOT.2021.3052066.
[69] Amin MM, Sutrisman A, Stiawan D, Ermatita E, Alzahrani MY, Budiarto R. Interoperability framework for integrated e-health services. Bulletin of Electrical Engineering and Informatics. 2020 Feb 1;9(1):354-61. doi: 10.11591/eei.v9i1.1825.
[70] Baskar S, Mohamed Shakeel P, Kumar R, Burhanuddin MA, Sampath R. A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications. Computer Communications. 2020 Jan; 149:17–26. doi: 10.1016/j.comcom.2019.10.004.
[71] Alhiyafi J. Health level seven generic web interface. Journal of Computational and Theoretical Nanoscience. 2018 Apr 1;15(4):1261-74. doi: 10.1166/jctn.2018.7302.
[72] Saripalle RK. Fast Health Interoperability Resources (FHIR): current status in the healthcare system. International Journal of E-Health and Medical Communications (IJEHMC). 2019 Jan 1;10(1):76-93. doi: 10.4018/IJEHMC.2019010105.
[73] Lim J, Zein R. The digital imaging and communications in medicine (DICOM): description, structure and applications. Rapid prototyping: theory and practice. 2006:63-86. doi: 10.1007/0-387-23291-5_3.
[74] Rouse M. SNOMED CT (Systematized Nomenclature of Medicine—Clinical Terms). SearchHealthIT. 2010.
[75] World Health Organization. ICD-11: International classification of diseases (11th revision).
[76] IEEE Standards Association [Internet]. IEEE Standards Association. Available from: https://standards.ieee.org/ieee/11073-10701/7538.
[77] Liu Q, Mkongwa KG, Zhang C. Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. SN Applied Sciences. 2021 Feb;3(2):155. doi: 10.1007/s42452-020-04058-2.

[78] Mazlan AA, Daud SM, Sam SM, Abas H, Rasid SZ, Yusof MF. Scalability challenges in healthcare blockchain system—a systematic review. IEEE access. 2020 Jan 24;8:23663-73. doi: 10.1109/ACCESS.2020.2969230.
[79] Navaz AN, Serhani MA, El Kassabi HT, Al-Qirim N, Ismail H. Trends, technologies, and key challenges in smart and connected healthcare. Ieee Access. 2021 May 11;9:74044-67. doi: 10.1109/ACCESS.2021.3079217
[80] Yang TH, Sun YS, Lai F. A scalable healthcare information system based on a service-oriented architecture. Journal of medical systems. 2011 Jun;35:391-407. doi: 10.1007/s10916-009-9375-5.
[81] da Silva Lisboa MF, Santos GL, Lynn T, Sadok D, Kelner J, Endo PT. Modeling the availability of an e-health system integrated with edge, fog and cloud infrastructures. In2018 IEEE symposium on computers and communications (ISCC) 2018 Jun 25: 00416-00421. IEEE. doi: 10.1109/ISCC.2018.8538589.
[82] Shukla S, Hassan MF, Khan MK, Jung LT, Awang A. An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PloS one. 2019 Nov 13;14(11):e0224934. doi: 10.1371/journal.pone.0224934.
[83] Mallick SR, Sharma S. Emri: A scalable and secure blockchain-based iomt framework for healthcare data transaction. In2021 19th OITS International Conference on Information Technology (OCIT) 2021 Dec 16 : 261-266. doi: 10.1109/OCIT53463.2021.00060.
[84] Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems. 2022 Apr 1;129:380-8. doi: 10.1016/j.future.2021.11.028.
[85] Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express. 2023 Aug 1;9(4):571-88. doi: 10.1016/j.icte.2023.02.007.
[86] Tahir A, Chen F, Khan HU, Ming Z, Ahmad A, Nazir S, Shafiq M. A systematic review on cloud storage mechanisms concerning e-healthcare systems. Sensors. 2020 Sep 21;20(18):5392. doi: 10.3390/s20185392.
[87] Khang A, Hajimahmud AV, Triwiyanto T, Abuzarova VA, Ali RN. Cloud Platform and Data Storage Systems in the Healthcare Ecosystem. In Medical Robotics and AI-Assisted Diagnostics for a High-Tech Healthcare Industry 2024: 343-356. doi: 10.4018/979-8-3693-2105-8.ch021.
[88] Awotunde JB, Bhoi AK, Barsocchi P. Hybrid cloud/Fog environment for healthcare: an exploratory study, opportunities, challenges, and future prospects. Hybrid artificial intelligence and IoT in healthcare. 2021:1-20. doi: 10.1007/978-981-16-2972-3_1.
[89] Sonune S, Kalbande D, Yeole A, Oak S. Issues in IoT healthcare platforms: A critical study and review. In2017 International Conference on Intelligent Computing and Control (I2C2) 2017 Jun 23: 1-5. doi: 10.1109/I2C2.2017.8321898.
[90] De Michele R, Furini M. Iot healthcare: Benefits, issues and challenges. In Proceedings of the 5th EAI international conference on smart objects and technologies for social good 2019 Sep 25 : 160-164. doi: 10.1145/3342428.3342693.
[91] Firouzi F, Farahani B, Barzegari M, Daneshmand M. AI-driven data monetization: The other face of data in IoT-based smart and connected health. IEEE Internet of Things Journal. 2020 Sep 30;9(8):5581-99. doi: 10.1109/JIOT.2020.3027971.
[92] Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated learning for healthcare informatics. Journal of healthcare informatics research. 2021 Mar;5:1-9. doi: 1007/s41666-020-00082-4.
[93] Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems. 2018 Nov 22;43(1). doi: 10.1007/s10916-018-1121-4.
[94] Ahmed SF, Alam MS, Afrin S, Rafa SJ, Rafa N, Gandomi AH. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion. 2024 Feb 1;102:102060. doi: 10.1016/j.inffus.2023.102060.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY