ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

The Internet of Things in Healthcare Services Transformation: Enhancing Through Applications, Data Security, Challenges and Future Innovations

Muhammad Dini Ibrahim[1]; Yahaya Salisu[2]; Usman Ibrahim Usman[3]; Fakhrun Jamal[4]; Nuraini Usman[5]

[1,2,3,4]Department of Computer Science and Engineering, Shobhit University, Meerut, Uttar Pradesh, India
[5]Department of International Programmes, Jigawa State Polytechnic for Information and Communication Technology (JSPICT), Kazaure, Nigeria

[1]ORCIDs: (https://orcid.org/0000-0001-8781-4899)
[2]ORCIDs: (https://orcid.org/0009-0007-8273-7119)
[3]ORCIDs: (https://orcid.org/0009-0001-6445-1973)
[4]ORCIDs: (https://orcid.org/0000-0003-0004-4882)
[5]ORCIDs: (https://orcid.org/0009-0008-4287-7456)

Publication Date: 2025/10/10

Abstract: The Internet of Things (IoT) makes it possible to bear and monitor objects remotely using communication devices over networks. Many patients encountered a lot of difficulties in medical facilities due to high chances of errors in medical treatments, which are caused by the lack of access to critical patient records, which are the pillars of medical diagnosis. The patient's records are typically stored in electronic medical records or paper-based records, making the retrieval of patient records challenging. Patients' interactions with physicians were previously limited to appointments, teleconferences, and text messages. Healthcare facilities lacked the means to track patients' health status and make timely recommendations. Smart devices, sensors, and connected devices continue to dynamically transform healthcare operations, supported by telemedicine and autonomous home support services for emergencies among the elderly and disabled, which are increasingly available. These methods are utilised to minimise physical contact, most especially in situations where the risk of viral contamination is high, such as care homes and infectious disease wards within hospitals, particularly during epidemics or pandemics. Through this research, we were able to provide significant insights into how IoT devices revolutionised the healthcare domain operational processes, identify some common challenges to optimise and protect patients' data and privacy across all platforms, also highlighted the innovative technologies mostly lightweight devices in tracking and monitoring health status of patients.

Keywords: *Internet of Things (IoT), Internet of Medical Things (IoMT), Artificial Intelligence, Remote Monitoring, Healthcare Devices, Healthcare Innovations.*

How to Cite: Muhammad Dini Ibrahim; Yahaya Salisu; Usman Ibrahim Usman; Fakhrun Jamal; Nuraini Usman (2025) The Internet of Things in Healthcare Services Transformation: Enhancing Through Applications, Data Security, Challenges and Future Innovations. *International Journal of Innovative Science and Research Technology*, 10(9), 2826-2837. https://doi.org/10.38124/ijisrt/25sep856

I. INTRODUCTION

While technological advancements in the field of science would not be able to stop the population from ageing or cure chronic diseases immediately, they make healthcare more affordable and accessible. The Internet of Things (IoT) is an innovation in the field of science and technology that has the potential to transform our interactions with our environments [1]. According to research findings in 2025, there will be more than 75 billion IoT devices connected globally [2]. The healthcare industry is one of the sectors that is expected to benefit significantly from this growth. Medical treatments of patients account for a significant portion of medical costs; medical inspection can be transferred from a

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

hospital (manual-based) to the patient's home by utilising IoT technology (smart home). Research has found that some of the effects on patients, as well as their caregivers and relatives, are due to a lack of adequate and timely medical knowledge sharing. Furthermore, several studies show that coordination of treatment among multiple providers is commonly flawed around the world, and medication errors are common.

IoT applications in healthcare industries, such as smart watches and sensors, enhance facilities and professional practice, bringing them out into the home, office, or social space. IoT enables medical practitioners to monitor their patients, individuals to track their own health, and service providers to deliver better treatment. However, one of the significant challenges of the healthcare industry is the acquisition of efficient and real-time information about patients. IoT devices come with numerous challenges, such as security, data breaches and vulnerabilities. This paper reviews various IoT devices used in the healthcare sector to monitor and capture patients' medical records, enhancing their health status remotely. This will help the medical practitioners and end users to utilise different IoT devices in the healthcare sector. Effective tracking of people and services is possible with the Internet of Things; by attaching sensors to patients, healthcare providers can use the Internet of Things to measure vital signs and other biometric information. Consequently, diseases and problems could be promptly detected. With the help of IoT, traffic signals can be controlled to help ambulances reach the hospital in time, by making emergency services more accessible to the people and saving lives.

The rest of this paper is organised in the following sections, as shown in Figure 1. Section II provides a definition as well as a systematic review of related literature on the application of IoT in healthcare systems. Section III gives a brief overview of the Application of IoT in Healthcare delivery solutions. Section IV presents a comparison of various healthcare IoT devices. Section V shows the integration of IoT with other technologies. Section VI shows a Comparison of IoT devices in the healthcare system, Section V shows common Cybersecurity attacks on IoT devices, Section VI presents an IoT data security mitigation strategy, Section VII shows IoT integration with emerging technology, and Section VIII shows different barriers and challenges of IoT in the healthcare system. Finally, Section IX provides the conclusion to the paper was not highlighted below but could be found at the end of this paper.

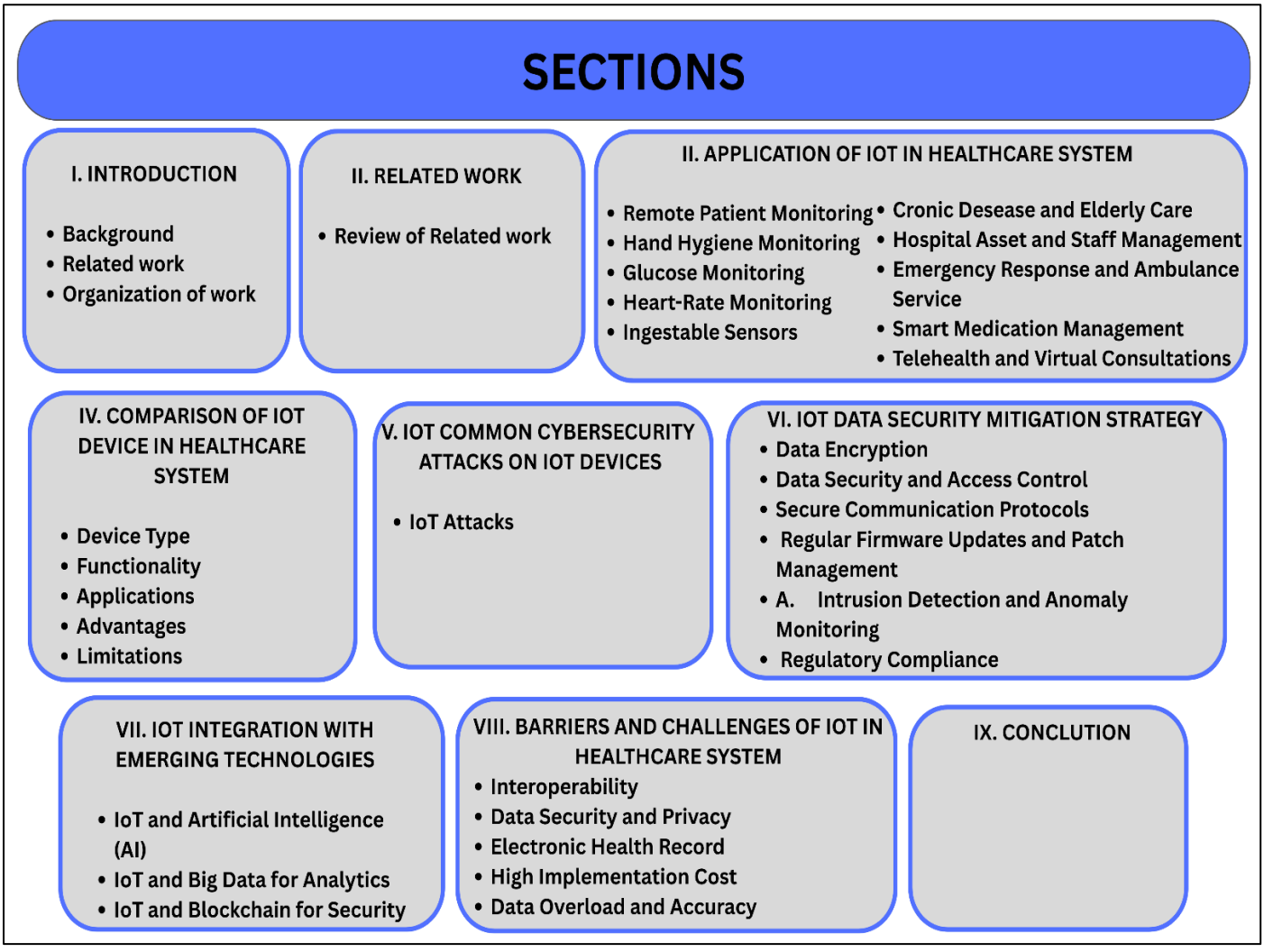

Fig 1 Organisation of Work

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

II. RELATED WORK

With the global advancement in technology, the healthcare industry has undergone significant changes, with the help of remote patient monitoring using IoT [3]. The Internet of Things (IoT) refers to a system of connected devices, objects, machines and people with unique identifiers that transmit data over a network without direct user interaction [4]. As the medical industry increasingly adopts advanced digital solutions, including IoT, Blockchain, AI and Cloud computing, the ability to continuously track real-time patients' medical status, examine potential causes of diseases, and optimise healthcare has improved significantly, by enhancing both patient outcomes and hospital efficiency [5]. Healthcare monitoring devices have been used as a groundbreaking method for tracking patients' health-related issues in real-time. This technology utilises wearable sensors to gather healthcare-related data, such as blood pressure, heart rate, and oxygen saturation levels. The data is mainly generated through Internet of Things (IoT) technology and examined by healthcare professionals to ensure precise diagnoses and prompt interventions during health crises [6].

The IoT describes the network of different interconnected physical objects that relate to software, sensors and other technological devices for connectivity and exchange of data with other devices over the internet. As the IoT device market grows rapidly, a particular concern is patients' data security and privacy [7]. A Medical facility equipped with IoT devices, such as smart wearable sensors [8], healthcare providers can periodically monitor patients' real-time health status and be alerted to any changes in patient activity. This can help reduce the effect of adverse reactions and improve patient outcomes. Confidentiality, Integrity and Availability (CIA) are crucial security goals in IoT. They ensure that data related to IoT devices is secured and unaltered by any unauthorised individual [9].

Patient remote monitoring in the healthcare sector is now largely owing to Internet of Things (IoT)-enabled devices, which can keep patients safe and secure while also inspiring physicians to provide superior treatment. Patient interest and satisfaction have also improved as interactions with doctors have become simpler and more efficient [10]. Furthermore, remote monitoring of patients tends to reduce hospital stays and prevent re-admissions. IoT has a positive effect on lowering healthcare costs and improving treatment outcomes. The innovative bed system is a specialised IoT bed that offers cutting-edge patient monitoring and care. In addition to tracking vital signs, monitoring heart rate, controlling temperature, and detecting falls or other changes in the patient's condition, smart beds may also identify whether a patient has turned or moved.

Furthermore, smart beds can be used to offer individualised support, comfort, and recovery. Remote management and control of innovative bed systems give caregivers more insight into a patient's status and enable them to act swiftly in case of any emergency. To further simplify patient care, smart beds can be linked to additional medical equipment like infusion pumps and oxygen monitors [11].

According to the World Health Organisation (WHO), research predicts that by the year 2050, over two billion people will be aged above 60 years. This signifies a huge threat to the global population as people become older. They are more vulnerable to chronic diseases and require more support [12]. As the worldwide population continues to evolve, many countries face numerous challenges in both public and private sectors. The healthcare system's Gross Domestic Product (GDP) of healthcare costs is expected to rise from 20 to 30% by 2050 [13].

III. APPLICATION OF IOT IN HEALTHCARE SOLUTION DELIVERY

A recent report revealed that the health sector has experienced a substantial transformation, as it was one of the first to adopt advanced mobile technology to boost productivity as well as provide on-demand services. Healthcare industries have overcome most of the challenges by gaining insight into the impact yielded by mobile-enabled gadgets. There have been numerous challenges in the health sector over the years, especially during the COVID-19 era, like limited physical operational time, remote locations, soaring overhead costs, and complex regulatory requirements, all of which have hindered their overall services. As one of humankind's most important aspects, the healthcare industry needed to overcome significant obstacles. Mobile system enables them with a systematic approach, which is also cost-effective [1].

Over the last few years, the use of IoT technology in healthcare has steadily progressed, placing powerful devices like smart insulin pens, smart watches, connected inhalers, asthma monitors, and more in the hands of patients, helping them to track their own health needs better, as well as rapidly access assistance if anything goes wrong. Wearable devices such as biosensors and smartwatches can also help healthcare professionals to remotely track and collect data on ongoing conditions, allowing observation and treatment that was previously only available in a hospital setting to take place anywhere. Some of the IoT Healthcare monitoring devices used to improve healthcare are mentioned below.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

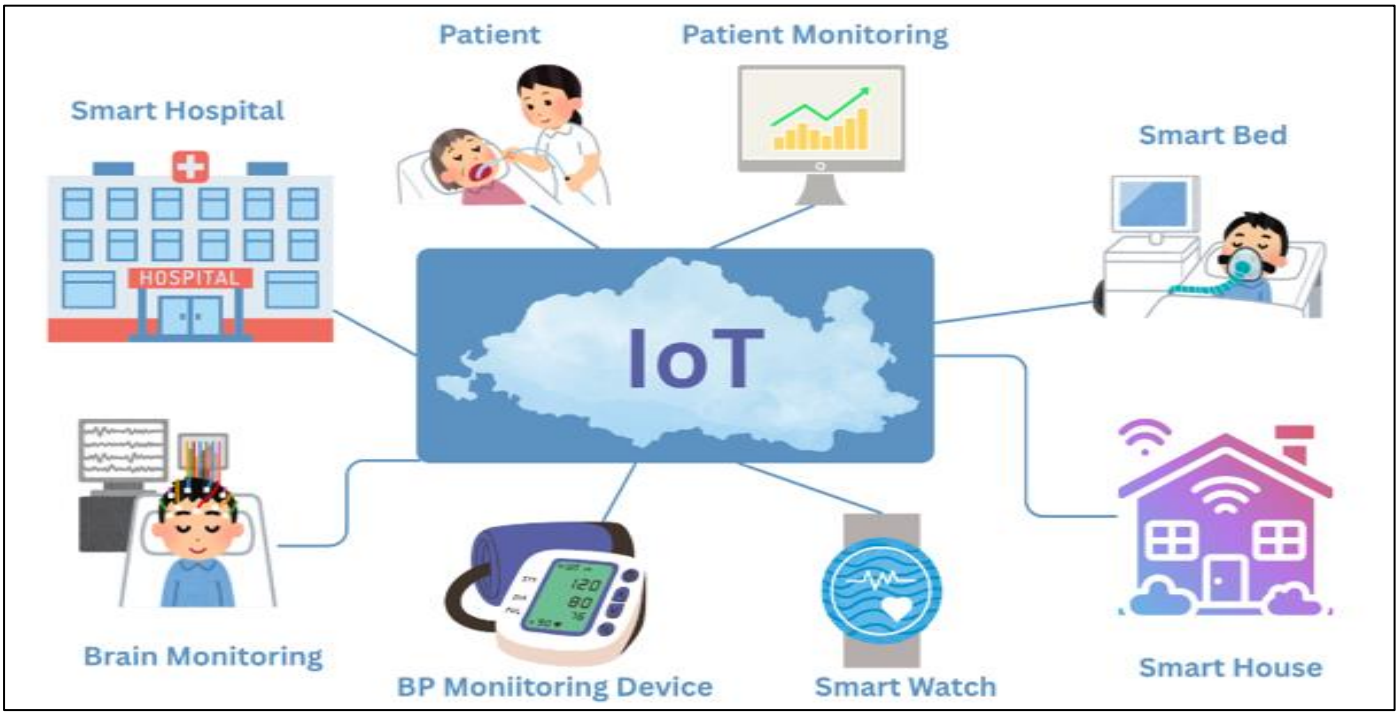

Fig 2 IoT Devices

➢ *Remote Patient Monitoring*

Remote patient monitoring is an advanced healthcare delivery that uses IoT (Internet of Things) to acquire patient data without the patient having to visit a hospital, which is the most common application of IoT devices for healthcare. RPM devices collect healthcare data such as heart rate, blood pressure, temperature, and other related data from patients who are not physically present in the healthcare facility, reducing the need for patients to drive to and from the facility for data collection [5].

When an IoT device gathers patient data, it sends it to a software program where it can be viewed by healthcare professionals or patients. These data are analysed and generate a report that can be used for treatment recommendations or precautions. An IoT sensor that senses a patient's unexpectedly low heart rate, for example, can send out an alarm so that medical staff can intervene. A major problem with remote patient monitoring systems is the data protection and privacy of the highly generated personal data that these IoT devices collect.

➢ *Hand Hygiene Monitoring*

Due to the high rate of potential transmission of COVID-19 and other infectious diseases through hand contamination, hand hygiene is a vital topic of discussion. There hasn't been a clear way to ensure that inside a healthcare facility, patients and technicians wash their hands regularly, hence reducing the risk of spreading infection to other people. Many hospitals, medical associations, and government entities also use numerous IoT devices to periodically remind people to wash their hands before entering hospital facilities or other public spaces to prevent further spreading of infectious diseases. The devices may also guide how to sanitise to reduce a specific risk for a particular patient [5].

Moreover, these machines are limited to warning people to clean their hands; they can't do it for them. Hence, research suggests that with the availability of these devices, the infection rate can be reduced by more than 60 per cent globally.

➢ *Glucose Monitoring*

The glucose monitoring device is an Internet of Things healthcare monitoring device that is used to measure the blood sugar levels of patients. The glucose monitoring device helps medical doctors to understand patients' levels of diabetes and the impact of various diets and drugs on their condition. The glucose monitoring device analyses a small sample of the patient's blood, typically from the tip of a finger. It enables patients to monitor their glucose levels, which medical practitioners can then use to analyse and conduct effective treatment to improve the patient's medical status. Traditional glucose monitoring has been inaccurate in recent years. Not only is the system's manual glucose level checking and recording process inconvenient, but it also only records a patient's glucose levels at the time the test is given. Periodic monitoring alone is insufficient to identify a problem if levels fluctuate widely. Moreover, despite the numerous advantages, glucose monitoring systems have several drawbacks, including low power storage, which necessitates a constant power supply. They are small enough to track continuously without affecting patients [14].

➢ *Heart-Rate Monitoring*

Heart rate, also called a heart detector, is a small IoT device that is used to monitor a patient's heart rate. The heart is a critical human body organ; even for patients in healthcare facilities, tracking heart rates can be difficult. Periodic heart rate checks do not protect against rapid heart rate variations, and standard hospital devices for continuous cardiac monitoring enable patients to be permanently connected to

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

wired machines, restricting their mobility. According to research, this device aims to produce ultra-accurate performance, which can be challenging to come by, but most modern systems can achieve accuracy rates of about 90% or better [15].

- *Chronic Disease and Elderly Care*

With the advent of IoT technology, the healthcare industry has drastically changed the way it administers care to patients, from early diagnosis to continuous medication and monitoring. In recent years patient needs to come to hospital physically to be diagnosed for various symptoms during consultation and post sample lab diagnosis, IoT as the game changer enable first level diagnosis and remote signal monitoring, chronic diseases that persist with old age like diabetes, hypertension, cardiac problem and asthma that their status is based on body conditions such as Fasting Plasma Glucose (FPG), Oral Glucose Tolerance (OGT), Random Plasma Glucose, Blood Pressure Readings, Lung Function, Electrocardiogram (ECG or EKG), Coronary Angiography, Blood Lipids(LDL) and, Echocardiogram, are now efficiently detected and monitored by IoT devices via sensors that transmits patient data to the cloud platforms which the healthcare personnel can access through digital interfaces enabling convenient delivery of service Another concerning health condition in elderly patients is accidental falls. In a recent study, the World Health Organisation (WHO) reported that approximately 684,000 disastrous falls occur each year, with most coming from elderly people. IoT Fall Detection Systems (FDS) assist in early signs of body system failure prior to potential falls [16].

- *Hospital Asset and Staff Management*

Running a modern healthcare centre is challenging with equipment, tools, and devices like wheelchairs, oxygen pumps, nebulisers, anaesthesia machines, and several personnel taking different shifts of duty across several wards, with some on the move for mobile services such as smart ambulance and first aid rescue. Cutting edge technology specifically IoT powered plays vital role in managing these assets efficiently by providing means of identifying and navigating exact position of assets within and outside hospitals, radio frequency identification system (RFID) a small taggable device with an in built chip set capable of emitting unique radio signals which is tagged on medical equipment/devices, the signal emitted is sensed by radio signal readers that are placed in strategic places around the hospital to assist in navigating the position of equipment/devices in the premise, Global Positioning System (GPS) on the other hand help with tracking medical facilities on the move outside the hospital like smart ambulance and patient intensive care system by synchronising with the terrain satellite to provide continues fleet feed on location data [17]. However, staff and patient records are frequently changing data that need careful management and efficient retrieval. Several solutions were designed to solve the problem, leveraging IoT end devices for data capture like personal digital assistants (PDAs), voice-to-EHR assistants (e.g., Nuance DAX), tablets and rugged mobile devices, and IoT-enabled staff monitoring via wearable badges and sensors to help management in staff workforce balancing[17], [18].

- *Emergency Response and Ambulance Services*

Mobile health care support ensures a first aid response to the victim at the incident place without waiting for a move to the hospital. Location tracking technologies such as GPS/GSM/GPRS and the HAT module as forms of wearable pieces of IoT devices enable location tracking of the victim, with the latter HAT module also used to send notifications via SMS to doctors/paramedics with the patient's health parameter history and current status to enable informed best decision-making in the case of abnormalities in past and current health status, also notifying relatives of the situation [18]. Furthermore, GPS with a predictive model is used in ambulance dispatch within the city and for pathfinding routes with the least traffic density [17].

- *Smart Medication Management*

A series of activities involved in Medication management, ranging from prescription, dispensing, administration, and monitoring to documentation, is optimised with tools such as smart medication dispensers, barcode scanning machines (patient wristband + drug label), and electronic medication administration records (EMAR) to limit errors and provide efficient delivery of service [17]. The smart pill dispenser is an IoT-enabled medication management system that has features like automated dosing reminders & alerts, a locking mechanism, connectivity, remote monitoring, and data logging designed to prevent errors in taking medicine and ensure the safety of the patient [19].

- *Telehealth and Virtual Consultations*

IoT enables telemedicine and virtual consultations with devices such as wearable RFID for patient body parameters such as heart rate, blood pressure, body temperature, SpO2, respiratory rate, ECG, and blood sugar, which are transmitted over the internet, which can be accessed by doctors/paramedics remotely IoT devices serve as a source of information for patient health parameter status when combined with widely adopted telemedicine platforms, such as Teladoc Health (USA), Amwell (American Well), Zoom for Healthcare (UK), Practo (India), and Babylon Health (UK). They help in reducing hospital congestion and waiting times, ensure 24/7 care accessibility, and support pandemic & emergency care scenarios [19].

IV. COMPARISONS OF IOT DEVICES IN HEALTHCARE

In Table 1 below, we compare different IoT devices that are used to provide support in enhancing patients' healthcare delivery services. The table consists of device type, functionality, applications, advantages, and limitations. This comparison table provides good explanations of various IoT devices to medical practitioners.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

Table 1 Comparison of IoT Devices

[Source] Device Type	Functionality	Application	Advantages	Limitations	Data Protection Status
[20] - Wrist-worn devices (Smartwatches, Fitness bands) - Patches -Smart garments - Rings Earphones	- Monitoring - Screening - Detection - Prediction	- Cardiovascular Health - Respiratory Health - Infectious Disease - Public Health - Chronic Disease Management - Personal Health Personalised and Preventive Care - Remote and Continuous Monitoring	- Improved Access - Large Scale Data Generation	- Data Quality Variability - Overestimation /Overprediction - Algorithmic Bias and Fairness. - Lack of Interoperability - User Interpretation and Anxiety	- Commercial Data Control - Lack of Transparency - Contextual Integrity - Surveillance Risks
[21] -Wrist-worn - Patches - Smart Garments - Rings - Motes/Sensor Nodes - Chest Straps - Insoles/Ankles Bands	- Monitoring - Screening - Detection - Prediction	- Chronic Disease Management - Cardiology Neurology	- Remote and Continuous Monitoring - Early Detection /Prediction - Patient Empowerment - Large-Scale Data Generation - Cost Reduction	- Data Quality and Variability - Clinical Accuracy - Better battery Life and Power Consumption Algorithmic Bias and Fairness	- Interoperability - User Dependency - Commercial Data Control - Lack of Transparency Security Vulnerability - Contextual Integrity Informed Consent
[22] - Wrist-worn - Patches - Smart Garments -Rings - Motes/Sensor Nodes - Chest Straps - Implantable - Specialised Medical Devices	- Monitoring - Screening - Detection - Prediction - Self-Management Support	- Chronic Disease Management - Cardiology - Respiratory Medicine - Prenatal Care - Neurology - Mental Health - Orthopaedic and Rehabilitation - Public Health	- Continuous Monitoring and Early - Intervention - Convenience and Access - Patient Empowerment and Education - Increased Confidence For Systems/ Practitioners - Personalised Care - Efficiency - Cost Reduction	- Data Quality Accuracy - Interoperability - Algorithmic Bias and Fairness User-Related Challenges - Digital Literacy and Usability - Patient Anxiety - Adherence Systemic Challenges - Increased Workload - Financial Barriers	- Commercial Data Control - Lack of Transparency - Security Vulnerabilities - Context Integrity - Constant Surveillance

V. COMMON CYBERSECURITY ATTACKS ON IOT DEVICES

The healthcare sector is a prime target for sophisticated cyberattacks; numerous healthcare infrastructures are targeted by attackers, exploiting vulnerabilities within systems or IoT devices. This kind of attack causes a lot of damage, disruption of services, data breaches and financial gain. Below are common types of attacks targeted at IoT-enabled healthcare environments that consist of attack type, description of attack and impact of attack to patients or infrastructures:

Table 2 IoT Attacks

Attack Type	Description	Impact
Man-in-the-Middle (MITM)	MITM attack intercepts data during transmission between IoT devices and servers.	-It causes Patient data leakage, -unauthorised control of devices.
Distributed Denial of Service (DDoS)	DDoS is a type of cyber-attack where an attacker sends an overwhelming request to a	-It causes disruption of critical healthcare services.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

	device/network to make the system services unavailable.	-It causes high traffic, leading to data loss and data compromise
Ransomware	Ransomware is an Unauthorised control of medical IoT devices (e.g., remote monitoring devices, insulin pumps) until a ransom is paid.	-It causes loss of access to medical records and puts patients' lives at risk. -It causes Potential patient harm or death. -financial loss
Data Breaches	Unauthorised access to patient health information (PHI).	-loss of patient trust and reputational damage -It causes legal liabilities.
Replay Attacks	A replay attack is the Reuse of intercepted data packets during transmission to impersonate legitimate data.	-It causes System confusion and inaccurate diagnosis or treatment.

VI. IOT DATA SECURITY MITIGATION STRATEGIES

Data security in IoT devices faces numerous cyber threats, which can cause data breaches and financial loss. IoT devices generate a huge amount of patient-related data every second. To ensure end-to-end security of IoT devices, there is a need for a multi-layered security approach:

➢ *Data Encryption*

IoT in healthcare relies on data generated from remote devices, which is transmitted to the cloud and other repositories or interfaces, making it prone to attacks such as ransomware, data breaches, eavesdropping, denial-of-service (DoS) attacks, malware, and botnets. Due to this factor, healthcare IoT has an increased attack surface, which compels the use of several techniques to encrypt and secure it, e.g., Advanced Encryption Standard (AES), PRINCE and XTEA, Elliptic Curve Cryptography (ECC), Blockchain-based Encryption, and Quantum Key Distribution (QKD). Additionally, protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are used to secure data in transit. These methods and protocols are implemented based on the different nature of the device, such as computing power and data transmitted. Moreover, it protects sensitive patient data from being intercepted or tampered with, thereby achieving compliance with regulatory bodies like HIPAA and GDPR [23], [24].

➢ *Authentication and Access Control*

Weak access credentials, such as weak usernames and passwords, are one of the setback features of IoT devices that are engineered cyber-threats, which gives attackers the advantage of performing attacks such as brute forcing to get an entry point and into the system for data breaches and other kinds of attacks. Multi-Factor Authentication (MFA) and access control mechanisms can be used to improve Data processing, storage, and transmission of IoT devices. Device-Specific Digital Identities (e.g., PKI), and Lightweight Authentication Protocols. Some may directly be suitable for low-power sensors [24]. Access control has to do with the permissions on what actions authenticated devices can perform, by limiting users/employees based on a predefined set of rules. Attribute-Based Access Control (ABAC), Network Segmentation, Zero Trust Architecture, and Blockchain for Access Management are among the strategies for deploying efficient access management in healthcare IoT network systems. They limit the risk of data alteration by granting access based on attributes, segmenting the network of devices with increased attack surfaces from the main hospital network, and providing a decentralised, immutable ledger for managing access [25].

- *Secure Communication Protocols*

Communication protocols are sets of rules governing interaction between two devices, like establishing sessions, encryptions, authentications, and integrity checks to ensure secure communication [26], moreover, multisensory interactions via state-of-the-art conceptual models Notably machine-to-machine (M2M) communication; These models leverage protocols like Constrained Application Protocol (CoAP) for constrained devices to request/respond similar to HTTP but more efficiently and with less power; Message Queuing Telemetry Transport (MQTT) for lightweight publish/subscribe protocol paired with transport layer security (TLS), ideal for low-bandwidth, low-power devices for wearable sensors; and Bluetooth Low Energy (BLE) for short-range communication, such as connecting a glucometer to a nearby smartphone or gateway. In essence, these protocols rely on various security mechanisms such as encryption, authentication, and integrity to function safely [23].

➢ *Regular Firmware Updates and Patch Management*

Foundational Cybersecurity practice for ensuring vulnerability is mitigated is regular firmware updates and patch management, they involve a systematic process of updating the low-level software (firmware) that controls the device hardware and applying patches, a small piece of code designed to fix a specific bug or vulnerability. Furthermore, it extends battery life, thereby adapting to evolving healthcare needs [23].

➢ *Intrusion Detection and Anomaly Monitoring*

Building resilience in healthcare IoT security encompasses the deployment of intrusion detection and anomaly monitoring for signature-based detection to identify known threats in the system and handle more subtle and complex threats, respectively. By integrating these methodologies, security teams can acquire a detailed perspective on the IoT ecosystem. When a device exhibits anomalous behaviour, the security system generates an alert, enabling the IT team to investigate and act before a data breach occurs, or patient care is compromised. This pre-emptive approach is crucial for maintaining the availability, integrity, and confidentiality of the IoMT [27]. IDS is of two categories. 1. Network-based (NIDS), which is placed at the strategic point of the network (e.g., at the gateway of the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

IoMT network) to monitor network traffic and identify threats of a known signature 2. Host-based (HIDS), which is installed directly on a specific medical device to identify threats that were not detected at the NIDS [28].

➢ *Regulatory Compliance*

Personal and healthcare data are patient vital information which he has rights over, the processing, disclosure, use and disposal of such information needs to follow a guideline of a specific regulatory framework, adhering to which ensures privacy, integrity and device safety. These regulatory frameworks are HIPAA (Health Insurance Portability and Accountability Act); HIPAA is a law that sets the standard for Protected Health Information(PHI), compliance with which is mandatory, GDPR (General Data Protection Regulation); GDPR is a European union law that protect the personal data of all EU citizens including health data as for ISO International Organization for Standardization/IEC International Electrotechnical Commission 80001; ISO/IEC is a technical standard risk management of IT networks that incorporate medical devices [23], [27], [29].

VII. IOT INTEGRATION WITH EMERGING TECHNOLOGIES

As the healthcare sector continues to evolve, numerous technologies have been integrated into different healthcare systems. Thus, advances in technology have enhanced how patients' record is collected, processed, stored and analysed. In this section, we try to highlight how IoT devices can be integrated with other advanced technologies, such as Blockchain technology, AI, and Big Data Analysis, to enhance the healthcare system.

➢ *IoT and Artificial Intelligence (AI)*

Artificial intelligence is revolutionising hospital operation through the development of algorithms and software that can work with little or no human intervention in different aspects of healthcare, like administration, diagnosis, treatment, medical imaging, drug formulation, and patient data management and processing, most of which are aided by IoT devices such as smart ECG monitors, remote patient monitoring systems (RPM), cloud-connected laboratory equipment, implantable cardiac devices (e.g., pacemakers with telemetry), and smart surgical instruments (robot-assisted), which enhances overall efficiency and optimises resource usage such as human resources. It also aids real-time patient monitoring, predictive analytics for early diagnosis, remote patient care and telemedicine, chronic disease management, automated emergency response systems, medication adherence tracking, data-driven clinical decision support, wearable health device optimisation, operational efficiency in hospitals, and epidemic outbreak prediction and monitoring [30]. Another notable implementation is on the wireless body area network and wearable network devices, which allow health monitoring systems to conduct real-time diagnosis, generation of alerts, and data analytics for future outbreak predictions in public health management [31].

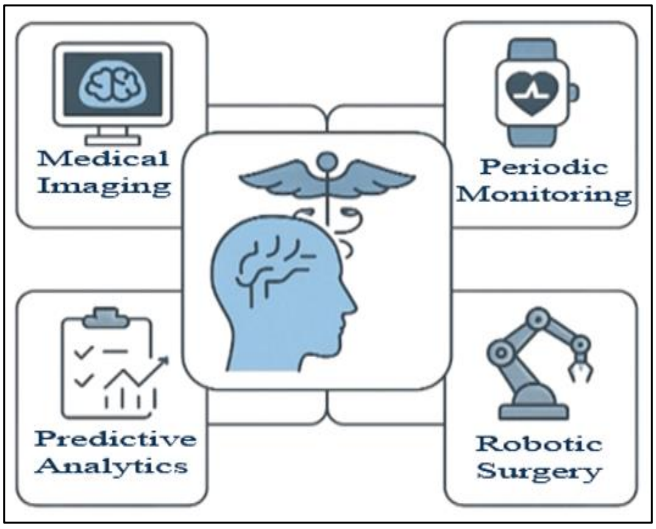

Fig 3 AI in Healthcare IoT

➢ *IoT and Big Data Analytics*

Every day in healthcare operation tremendous voluminous amount of data is being generated from different sources of input mostly IoT clinical equipment and devices such as AI-powered imaging devices (MRI, CT with cloud access), Wearable fitness trackers (e.g., Fitbit, Apple Watch), which is stored across diverse repositories example cloud storage and is processed by distributed computing system like Apache Hadoop or Spark platforms because it is not possible to access and process by the traditional data processing systems such as Database Management Systems (DBMS), this enable healthcare professionals to have overall or timely insight of health condition of individual patients, and allows informed decision, often predictive models process vital patient records to predict outbreak [32]. Another proposed mobile cloud computing model aims to facilitate decision making by classifying medical records before uploading data to the cloud, where supervised and unsupervised machine learning algorithms will process to identify medical conditions and propose treatment[33].

➢ *IoT and Blockchain for Security*

Distributed ledger technology (DLT) is used by blockchain technology to provide an immutable, decentralised and transparent mechanism to protect sensitive healthcare data generated by Internet of Medical Things (IoMT). With these decentralise temper proof technology of records (i.e., Blockchain) IoMT vulnerability such as constant connectivity, large attack surface, and weak device security that made it prone is neutralised or prevented by secure data sharing, device authentication, and end-to-end encryption ensuring integrity, traceability, and trust in IoMT networks, with the help of blockchain IoMT will be regulated and compliant to HIPAA and GDPR[34], [35].

VIII. BARRIERS AND CHALLENGES OF IOT IN THE HEALTHCARE SYSTEM

The role of the Internet of Things (IoT) has been illustrated, and it is revolutionising the healthcare sector. IoT devices are introducing new development and modular systems into the health care industry, whether it's remote

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

patient control, ingestible sensors, hand hygiene, or mobile health applications. Regardless, every study ends with a challenge. It's all well and good to show the impact of wearable technology and computers that can simplify clinical practices when it comes to IoT in healthcare, but what are the difficulties involved in handling the devices? Here are three obstacles to the successful use of IoT health devices, as well as how to overcome them.

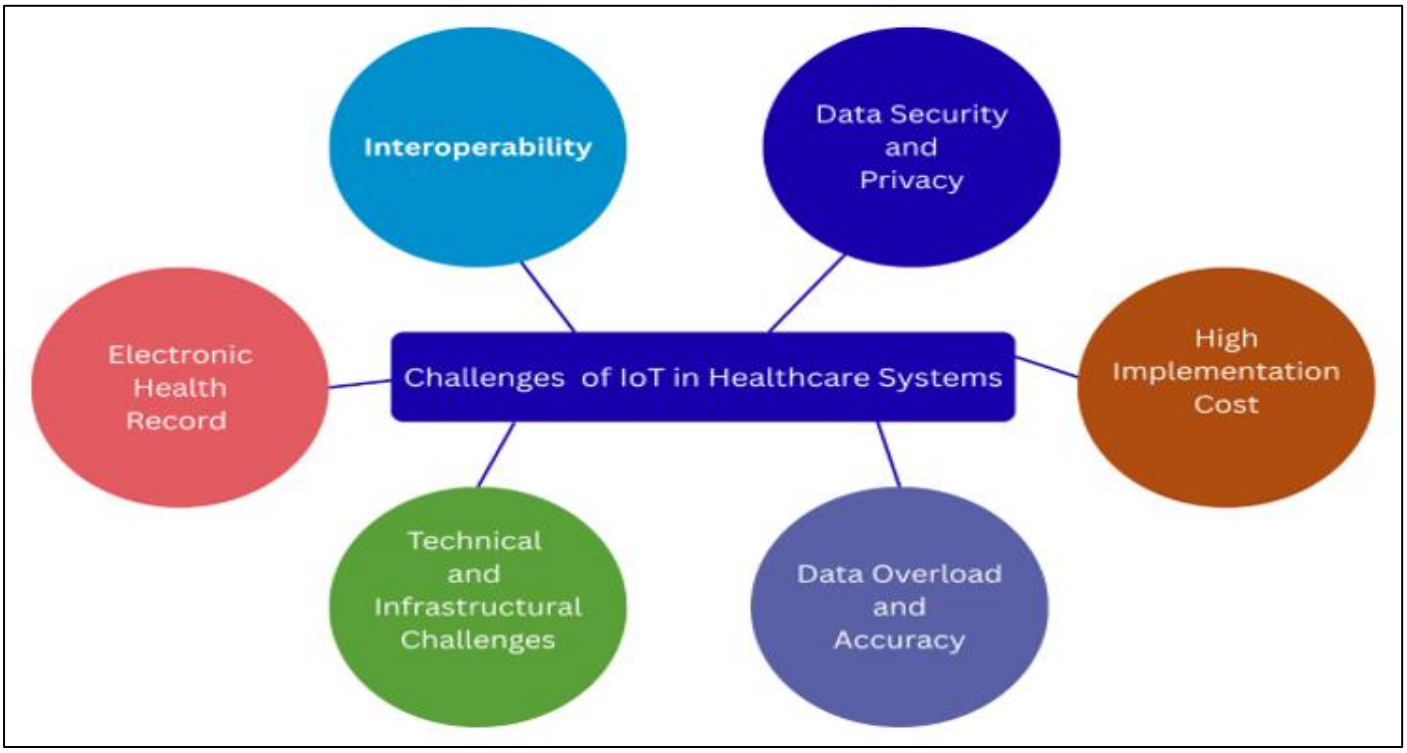

Fig 4 Challenges of IoT in Healthcare Systems

➢ *Interoperability*

Interoperability is one of the most difficult challenges of integrating IoT in health care. IoT devices cannot reliably exchange data with the required departments. Data from an asthma monitoring system is directly sent to the patient's doctor, rather than to their primary care physician. Hence, this leads to a greater gap in data operability. Furthermore, another significant challenge is keeping track of patients' smart devices and ensuring that they are maintained after they are discharged from the hospital. Without proper awareness of the IT department, the medical staff can send a patient home with an IoT device without an appropriate understanding of how to maintain its optimal operation.

Hence, choosing a well-skilled IoT Expert who offers robust application integration is a key solution to the above problems. Applications from various manufacturers can interact as a distributed system, allowing healthcare management to monitor and maintain them using appropriate technology and components. Interoperability in the healthcare sector can be improved by implementing a robust interface between the different IoT devices.

➢ *Data Security and Privacy*

Another significant challenge posed by IoT, particularly in healthcare, is Data Security and Privacy. IoT devices collect numerous data in real-time, but most of this data lacks adequate protocols and standards. There is considerable controversy surrounding data integrity and control. Therefore, data stored in IoT devices is prone to data breaches, making it more vulnerable to cybercriminals who might exploit the IoT devices and steal confidential information. Data Impersonation and the development of fake IDs are two examples of IoT data security and privacy challenges.

Furthermore, the integrity of the data provided by the IoT is questionable. An IoT device can be coupled with Blockchain technology to improve data security by providing high-level data encryption methodology, for example, and an IoT device can be integrated with blockchain technology (Smart contract) to grant or block device access based on organisational security assessments. By integrating blockchain technology (smart contract), IoT networks can enforce strict security policies and mitigate the risk of data breaches [36].

Another key solution to deal with IoT data security problems is to move some or all of the IoT-related operations to the cloud. A good cloud provider, like Microsoft Azure, can handle high data operations and high data security, so businesses don't have to worry about keeping their own data centre safe.

➢ *Electronic Health Record*

Another critical challenge of IoT in Data Integration is that it's vital and challenging to collect data from a variety of IoT monitoring devices and integrate it into a patient's electronic health records (EHR). These data must integrate seamlessly with the EHR. Data from wearable and other

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

smart devices often gets stuck in a vendor's apps or repository. Hence, these data can be contained in a patient's medical history, where doctors can see it and act on it.

This connectivity issue can be resolved by APIs and microservices, which enable secure connections between multiple applications. An enterprise service bus can be used by any application to connect to any data source.

➢ *High Implementation Cost*

IoT implementation cost is one of the most significant problems when thinking about IoT creation as a service for remote healthcare solutions. But if the IoT implementation fixes healthcare problems, the costs are worth it. It will take a lot of time and resources to develop an IoT device, but the benefits of utilising IoT will be huge. The organisation will save time and manpower while improving business processes, creating new revenue streams, and opening up new business opportunities.

➢ *Data Overload and Accuracy*

Electronic health records (EHRs), smart devices, and other linked medical equipment produce enormous amounts of data in the healthcare ecosystem as a result of the advancements in the healthcare setting. This data is therefore essential for data analytics and real-time decision-making, but it can also lead to data overload. Sorting through this massive amount of data to find helpful insights can be difficult for healthcare professionals. Data management in healthcare is a crucial concern in delivering healthcare services. Inaccurate data from device failure, sensor drift, signal noise, or incorrect user input can lead to incorrect medical diagnosis, inappropriate treatment, and compromised patient safety.

Additionally, the lack of standard formats and protocols among different IoT devices may pose another challenge. Implementation of AI-powered analytics and Effective data management solutions, such as data aggregation frameworks and real-time alerting systems, is essential to minimise these problems. Still, they must be carefully designed to ensure clinical relevance, minimise false alarms, and reduce the cognitive burden on medical staff [15].

➢ *Technical and Infrastructural Challenges*

With the advent of technical infrastructure, such as reliable network access, enough data storage, cloud computing capabilities, and a secure network, the deployment of IoT devices in healthcare is crucial. Different healthcare facilities lack the availability of resources needed to support the deployment of IoMT-based healthcare delivery systems, particularly those located in underdeveloped communities.

- *Technical Challenges Include:*

✓ Smart device Interoperability issues: Compatibility issues between devices from different manufacturers.
✓ Latency and bandwidth limitations: A lack of consistent Latency and limited bandwidth can hinder real-time monitoring and emergency response to critical health-related challenges.
✓ Power consumption: With the current advancement in battery systems, there are a lot of concerns for battery-dependent wearable devices and power consumption among different IoT devices.
✓ Scalability: There is a significant demand for the scalability of systems as the number of connected devices and patients increases globally.

Furthermore, many healthcare systems may not always have the high level of technical expertise needed to maintain fully functional IoT-based healthcare systems. The ongoing requirement for cybersecurity awareness, software upgrades, and system maintenance further increases the operational complexity. To overcome these obstacles, healthcare organisations and IT providers must work together to ensure the seamless and long-term integration of IoT solutions, optimise IT infrastructure, and train healthcare personnel in fundamental IT requirements [10].

IX. CONCLUSION

The field of IoT is rapidly transforming the healthcare industry by providing emerging technologies to monitor, maintain, and manage health-related demands. However, there are still emerging challenges that need to be addressed urgently. This paper on the role of IoT in optimising healthcare services and its applications provides an overview of different aspects of IoT in the healthcare system. It addresses some of the significant IoT healthcare advantages and their shortcomings for the public. In conclusion, with rapidly evolving innovations and technical progressions such as remote sensing, communication development, and the overwhelming amount of data generated through IoT, it has become a significant aspect of our lives. This will undoubtedly promote lifestyle and healthcare industry developments. Although the Internet of Things is impacting health care, it is far from ideal. To summarise the content, IoT in healthcare is far from definitive.

Further research and development are needed to fully exploit IoT's benefits and make healthcare more accessible and effective. The study should focus on the challenging areas I described in the challenge segment and find appropriate solutions. In this age of global transformation and soon, I assume that with the implementation of more smart devices, healthcare will become smarter, and current issues will be resolved. With the help of IoT, medical advances will be made, and everyone will be able to benefit. IoT has the potential to improve the healthcare system globally, but proper study and innovation are needed, especially in Data Security and privacy.

REFERENCES

[1]. V. A. Dang, Q. Vu Khanh, V.-H. Nguyen, T. Nguyen, and D. C. Nguyen, "Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity," Sensors, vol. 23, no. 9, p. 4200, Apr. 2023, doi: 10.3390/s23094200.
[2]. D. Shehada, A. Gawanmeh, C. Y. Yeun, and M. Jamal Zemerly, "Fog-based distributed trust and reputation

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

management system for internet of things," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 10, pp. 8637–8646, Nov. 2022, doi: 10.1016/j.jksuci.2021.10.006.

[3]. M. Al-rawashdeh, P. Keikhosrokiani, B. Belaton, M. Alawida, and A. Zwiri, "IoT Adoption and Application for Smart Healthcare: A Systematic Review," Sensors, vol. 22, no. 14, p. 5377, July 2022, doi: 10.3390/s22145377.

[4]. M. J. Kang and Y. C. Hwang, "Exploring the Factors Affecting the Continued Usage Intention of IoT-Based Healthcare Wearable Devices Using the TAM Model," Sustainability, vol. 14, no. 19, p. 12492, Sept. 2022, doi: 10.3390/su141912492.

[5]. S. Tiwari, K. Nahak, and A. Mishra, "REVOLUTIONIZING HEALTHCARE: THE POWER OF IOT IN HEALTH MONITORING".

[6]. Z. Cekerevac, S. Ohrimenco, and P. Cekerevac, "Protecting Blockchain from IoT Device Attacks: Challenges and Solutions," MEST J., vol. 13, no. 2, pp. 81–93, July 2025, doi: 10.12709/mest 13.13.02.05.

[7]. A. Andrews, G. Oikonomou, S. Armour, P. Thomas, and T. Cattermole, "IoT Device Identification Techniques: A Comparative Analysis for Security Practitioners," IEEE Access, vol. 13, pp. 82610–82620, 2025, doi: 10.1109/access 2025.3568673.

[8]. M. Maddeh, F. Hajjej, M. B. Alazzam, S. A. Otaibi, N. A. Turki, and S. Ayouni, "Spatio-Temporal Cluster Mapping System in Smart Beds for Patient Monitoring," Sensors, vol. 23, no. 10, p. 4614, May 2023, doi: 10.3390/s23104614.

[9]. P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives," J. Food Qual., vol. 2021, pp. 1–20, May 2021, doi: 10.1155/2021/7608296.

[10]. M. Shamir and R. Spunda, "The Role of Blockchain in Securing IoT Devices and Critical Infrastructure," 2025, Unpublished. doi: 10.13140/RG.2.2.35259.73769.

[11]. S. Ayouni, M. Maddeh, S. Al-Otaibi, M. B. Alazzam, N. Alturki, and F. Hajjej, "Development of a Smart Hospital Bed Based on Deep Learning to Monitor Patient Conditions," J. Disabil. Res., vol. 2, no. 2, July 2023, doi: 10.57197/jdr-2023-0017.

[12]. M. N. Alkhomsan, M. A. Hossain, Sk. Md. M. Rahman, and M. Masud, "Situation Awareness in Ambient Assisted Living for Smart Healthcare," IEEE Access, vol. 5, pp. 20716–20725, 2017, doi: 10.1109/ACCESS.2017.2731363.

[13]. H. H. Mohamad Jawad, Z. Bin Hassan, B. B. Zaidan, F. H. Mohammed Jawad, D. H. Mohamed Jawad, and W. H. D. Alredany, "A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations," Electronics, vol. 11, no. 19, p. 3223, Oct. 2022, doi: 10.3390/electronics11193223.

[14]. T. Manyazewal et al., "Digital continuous glucose monitoring systems for patients with HIV-diabetes comorbidity in Ethiopia: a situational analysis," Sci. Rep., vol. 14, no. 1, Nov. 2024, doi: 10.1038/s41598-024-79967-y.

[15]. D. N. Venu, D. A. ArunKumar, and K. K. Vaigandla, "Investigation on Internet of Things(IoT) : Technologies, Challenges and Applications in Healthcare," no. 2236.

[16]. M. E. Karar, H. I. Shehata, and O. Reyad, "A Survey of IoT-Based Fall Detection for Aiding Elderly Care: Sensors, Methods, Challenges and Future Trends," Appl. Sci., vol. 12, no. 7, p. 3276, Mar. 2022, doi: 10.3390/app12073276.

[17]. K. Saritha et al., "IoT enabled hospital asset tracking using advanced interdisciplinary approaches," E3S Web Conf., vol. 507, p. 01007, 2024, doi: 10.1051/e3sconf/202450701007.

[18]. B. G. Mohammed and D. S. Hasan, "Smart Healthcare Monitoring System Using IoT," Int. J. Interact. Mob. Technol. IJIM, vol. 17, no. 01, pp. 141–152, Jan. 2023, doi: 10.3991/ijim.v17i01.34675.

[19]. B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," J. Healthc. Eng., vol. 2021, pp. 1–18, Mar. 2021, doi: 10.1155/2021/6632599.

[20]. S. Canali, V. Schiaffonati, and A. Aliverti, "Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness".

[21]. E. Escobar-Linero, L. Muñoz-Saavedra, F. Luna-Perejón, J. L. Sevillano, and M. Domínguez-Morales, "Wearable Health Devices for Diagnosis Support: Evolution and Future Tendencies".

[22]. L. P. Serrano et al., "Benefits and Challenges of Remote Patient Monitoring as Perceived by Health Care Practitioners: A Systematic Review".

[23]. R. Amini Gougeh and Z. Zilic, "Systematic Review of IoT-Based Solutions for User Tracking: Towards Smarter Lifestyle, Wellness and Health Management," Sensors, vol. 24, no. 18, p. 5939, Sept. 2024, doi: 10.3390/s24185939.

[24]. J. V., V. Balan, and B. V. S., "Security Issues in IoT: Perspective Review," Comput. Netw. Commun., pp. 101–117, Mar. 2025, doi: 10.37256/cnc.3120256140.

[25]. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," Sensors, vol. 20, no. 17, p. 4828, Aug. 2020, doi: 10.3390/s20174828.

[26]. S. Abdulmalek et al., "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review," Healthcare, vol. 10, no. 10, p. 1993, Oct. 2022, doi: 10.3390/healthcare10101993.

[27]. K. Svandova and Z. Smutny, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," J. Multidiscip. Healthc., vol. Volume 17, pp. 2281–2301, May 2024, doi: 10.2147/JMDH.S459987.

[28]. A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities,"

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep856

Artif. Intell. Rev., vol. 58, no. 4, p. 114, Jan. 2025, doi: 10.1007/s10462-024-11101-w.

[29]. Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh, "DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS," Comput. Sci. IT Res. J., vol. 5, no. 3, pp. 528–543, Mar. 2024, doi: 10.51594/csitrj.v5i3.859.

[30]. "A systematic literature review of artificial intelligence in the healthcare."

[31]. S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review," IEEE Sens. J., vol. 21, no. 22, pp. 24920–24932, Nov. 2021, doi: 10.1109/jsen.2021.3055618.

[32]. "Internet of Things and Big Data Analytics in Preventive."

[33]. L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications," IEEE Access, vol. 4, pp. 6171–6180, 2016, doi: 10.1109/access.2016.2613278.

[34]. Y. Y. Ghadi et al., "The role of blockchain to secure internet of medical things," Sci. Rep., vol. 14, no. 1, p. 18422, Aug. 2024, doi: 10.1038/s41598-024-68529-x.

[35]. A. H. Allam, I. Gomaa, H. H. Zayed, and M. Taha, "IoT-based eHealth using blockchain technology: a survey," Clust. Comput., vol. 27, no. 6, pp. 7083–7110, Sept. 2024, doi: 10.1007/s10586-024-04357-y.

[36]. Umair Zafer and J. Pomeroy, "Blockchain-Powered IoT Security: Ensuring Data Integrity and Device Trustworthiness," 2025, Unpublished. doi: 10.13140/RG.2.2.15756.22404.