CHAPTER 1

Introduction

When we discuss the "Internet of Things," we're referring to a situation in which common objects have Internet-connected sensors, microcontrollers, and transceivers to enable two-way communication. By equipping these things with the proper protocol stacks, they may communicate with one another and with people, transforming them into an integral part of the Internet. The internet currently has a significant impact on many facets of the potential user's daily life. With the intention of employing sensor technology to connect any and all physical items to the Internet, several (IoT)-based apps have been created. By utilising IoT solutions, it may be possible to improve healthcare costs, access to care, and care quality. Wellness, medical treatment, and emotional support provided to an individual are said to be "personalized" when they take into account the person's unique genetic makeup, personality, and background. The healthcare tenet of "the appropriate therapy for the right person at the right time" empowers people, produces more desirable results, increases patient happiness and lowers medical expenses. An effective healthcare system would put homecare, early pathology diagnosis, and prevention ahead of expensive clinical therapy. Protecting each person's unique digital identity is one way that IoT ensures healthcare can be delivered in a tailored manner.

Conventional healthcare institutions have misdiagnosed a number of health issues due to a lack of easily accessible healthcare remedies. However, quick monitoring and analysis of patient data are now possible thanks to sophisticated, pervasive Internet of Things-based sensors. Real-time medical data is gathered, processed, and uploaded to the cloud for storage, analysis, and alert generating using an IoT-based healthcare system. This innovative method of data collection allows for widespread, constant access to medical equipment through the Internet. In India, researchers analyzed the effectiveness of hospitals and clinics by looking at how they used it to better serve their patients. Patient records were found to be badly kept at several hospitals, with many patients being transferred between facilities based only on paper records. Due to a lack of resources, the quality of care given to patients was worthless. Based on the findings, electronic health records and other forms of IT might help improve healthcare institutions (EHRs). Using electronic health records (EHRs) is less prevalent and more prone to mistakes, according to the survey, because of how complicated it is. In this research, we propose WebEHR, a

user-friendly and effective Employable EHR (EEHR) [1] system. This approach uses the internet to facilitate communication across various medical institutions, which in turn facilitates the upkeep and distribution of relevant data. The ability to get medical treatment is a must for everyone. In spite of this, not every patient is treated equally by the physicians in terms of treatment and remuneration. Another problem with the healthcare system is that there aren't enough hospitals and clinics to look into a patient's past and present conditions to determine the best course of treatment. As a result, the healthcare system's effectiveness needs to be increased [2]. This study suggests merging all hospital records, no matter how many or little, using a cloud-based method so that patient data can stay in one place. By using this strategy, the dominance of for-profit hospitals would be diminished and patients would be guaranteed of receiving fair treatment in public facilities. Deterioration in patients' clinical status is a major problem in healthcare facilities [3]. This research paper explains how hospitals might benefit from wireless patient monitoring. Patients' heart rates and oxygen saturation levels are monitored continuously by the wirelessly connected devices. WSNs' potential use in healthcare settings like hospitals are discussed as well.

The success of India's healthcare system may be directly traced to the country's highly qualified medical personnel. Initiatives have been conducted to improve healthcare quality [4]. This article explores the outcomes of recent attempts to improve the healthcare system. What has to be done to improve the quality of India's medical services is also addressed, as there is an issue of a lack of safety measures for medical equipment. Telehealth networks are required because of the ageing population and the incidence of numerous chronic disorders [5]. It gives a comprehensive analysis of the potential of wearable technology in telemedicine. This system's main goal is to do tele-home patient monitoring through the use of wireless connections, wearable technology, and other sensors. According to the survey, health issues, such as heart conditions or other major health issues, are the main reason behind traffic accidents in India [6]. In order to prevent vehicular mishaps and ensure the driver has prompt access to medical care, a sophisticated monitoring system is recommended. Using a smart phone, this setup transmits data about the user's vital signs to a remote server. Wireless sensor networks can now be used in the healthcare industry due to advancements in a network with low power architecture and medical sensors [7]. It describes various application possibilities for the healthcare industry, difficulties presented by WSNs, privacy protections for private medical information, and research questions. Mobile computing, medical sensor technology, and

communication systems are all combined in m-health [8]. Various wireless technologies discussed are GPRS, WLAN, ZigBee, and Bluetooth. They also include various difficulties and potential implementation problems for a range of use cases, all from the perspective of healthcare.

Wearable technology has become more common in the medical industry dramatically in recent years. The majority of the body's medical monitoring technology used today is cumbersome and uncomfortable to wear [9]. By combining the electrocardiogram (ECG), accelerometer, and oxygen saturation (SpO2) sensors into a single device, it contributes to the development of user-friendly medical equipment. Each physical object in the Internet of Things, a computer process, has one or more sensors, microcontrollers, and transceivers attached to them so that data may be collected and transmitted from them. It is a crucial part of the Internet since it was created with the right protocol stacks that allow objects to connect with one other and with people [10]. Consumer viewpoint for IoT applications include e-health, smart homes, assisted living, smart meter's, security monitoring, and remote data monitoring and control [11]. "The Internet" as we know it has significantly changed as a result of IoT. In the not-so-distant in the future, billions of gadgets will be linked and capable of speaking to one another automatically, producing large volumes of data that provide humans access to information and enable them to remotely control a variety of apparatus [12]. However, it has two significant drawbacks: a short battery life and related delays in the IoT, also referred to as the Internet of Things. Connecting real-world things to the internet is the goal of the Internet of Things (IoT) concept [42]. These concepts are relevant to any web applications and may be used in IoT projects. The "IoT" is the name of the network of connected devices in the future. A network called the Internet of Things (IoT) allows for direct connection with actual objects. It highlights the IoT's numerous components and features as well as its numerous practical and social advantages.

Among the many applications for wireless sensor networks, disaster management, event monitoring, and precision agriculture are just a few. Installing a gateway is an option if you want internet access to your WSN data [15]. Through the IP protocol (IP), WSNs and the Internet are connected. The effort that went into creating an IoT using WSN standards and technology is described. IoT applications including smart homes, healthcare, industrial automation, etc. frequently employ the ZigBee protocol. Only two of the many wireless communication technologies readily available today are Bluetooth and 802.11. These wireless networks are nevertheless plagued by a number of fundamental problems,

including scalability and power consumption. The shortcomings of Bluetooth and WLAN are addressed by the advent of ZigBee [16]. ZigBee is perfect for low-speed wireless personal area networks because to its cheap cost and power consumption.

The fact that end devices can operate in sleep mode contributes to this low power usage. Numerous technology-based healthcare application options are available in the IoT sector. The optimal plan of action must be selected among the available possibilities taking into account the limitations and priorities specific to the application [17]. In order to create cost-effective Health-IoT systems that enhance relevant medical services, clinical care, and remote monitoring to handle new challenges, it examines structured system engineering techniques. IoT is becoming more and more significant in the healthcare industry to improve patient access to care, elevate the standard of care, and—most importantly—reduce costs. [18-19]. ZigBee's low cost and low power consumption make it ideal for low-speed wireless personal area networks. The principles of IoT and how it works with wireless and sensor technologies to execute the intended healthcare applications were summarised in this study. Medical information system development is significantly impacted by IoT-based healthcare systems. It's critical to track and monitor patients' locations to enhance healthcare delivery. Unfortunately, these demands cannot be meaningfully satisfied given the state of healthcare today and the associated limitations of medical technology. This study's main focus is on how IoT functions in the healthcare system, but it also discusses its contributions to other fields of study and covers its present applications. One of the IoT's many applications is the delivery of healthcare [20]. It examines the many IoT-based healthcare network platforms, applications, and commercial trends as well as the technological improvements and advances in this area. It also addresses a variety of security issues and offers a sophisticated security strategy for minimising risks. It is possible to connect medical devices to open networks like the Internet with the aid of numerous commercially available solutions [21]. The issue at hand, however, is figuring out how to ensure the confidentiality of personal medical information. Additionally, it analyses the advantages and disadvantages of eHealth services developed via the Internet of Things.

1.1 Motivation

Here are some reasons for securing healthcare IoT. Device security is a major challenge for users when new technologies are implemented in the healthcare industry. IoT in healthcare highlights two crucial communication-related aspects: Latency and traffic. For

instance, when traffic congestion is reduced, latency decreases proportionately. This is still the primary focus of most studies, particularly during emergencies. This is due to the fact that any delay in response or communication will be negative impact on the patient.

1. **Safe and Reliable Healthcare Environment**: It Promotes Better Patient Outcomes and Experiences: Giving security in healthcare IoT top priority fosters trust and confidence among patients, healthcare providers, and stakeholders.
2. **Patient Privacy and Confidentiality**: Protecting patient privacy in the healthcare industry involves securing the Internet of Things to ensure the confidentiality of patient information and its protection against breaches or intrusions.
3. **Data Integrity**: Preserving the accuracy, dependability, and integrity of medical data is essential for preserving the standard of patient care and treatment. This can be achieved by protecting the integrity of healthcare IoT systems.
4. **Prevention Against Cyberattacks**: Health care data security and integrity are guaranteed by blockchain's decentralized architecture processes, which make it inherently immune to these kinds of attacks and drastically lower the chance of data breaches.
5. **Efficiency and Cost Reduction**: Health care data security and integrity are guaranteed by blockchain's decentralized architecture processes, which make it intrinsically immune to these kinds of attacks and drastically lower the chance of data breaches.

1.2 Challenges

The following is a list of challenges that are faced while designing healthcare system ,

1. **Security and privacy**: One of the greatest issues with safe IoT for healthcare is One of the primary issues with secure healthcare IoT is ensuring that patient data is kept secure and private. Data breaches and hacking may occur on IoT devices, which could have a negative impact on patient privacy and safety.
2. **Interoperability**: Integrating various healthcare IoT systems and guaranteeing smooth data sharing between numerous stakeholders, platforms, and devices.
3. **Standards and regulations**: For secure healthcare IoT, there are currently no global standards or laws, which might cause inconsistencies and misunderstanding over how devices and systems should be created and used.

4. **Integration with existing systems**: It could be challenging and time-consuming to integrate new IoT devices and systems with existing patient monitoring and care systems used by many healthcare organizations.
5. **Data management and analysis**: It can be difficult, especially in real-time, to handle and analyze the vast amounts of data generated by secure healthcare IoT devices examine the enormous volumes of data produced by safe Internet of Things medical devices.
6. **Scalability**: Designing a healthcare system that can accommodate increasing patient volumes, technological advancements, and evolving healthcare needs without compromising performance or quality of care.

1.3 Problem Definition

In order to construct an irreversible and transparent ledger for storing sensitive patient health data, blockchain technology must be included in the design and implementation of a safe health monitoring system for Internet of Things networks.

Blockchain integration enhances data security, privacy, and trust in healthcare systems, promoting better patient outcomes and compliance with regulatory requirements.

Distribute health data across multiple nodes in the blockchain network to prevent a single point of failure and enhance resilience against cyber-attacks. Every node keeps a duplicate of the blockchain ledger, ensuring redundancy and availability of data even in the event of node failures or network disruptions.

IoT scenarios based on blockchain that are secure for the healthcare industry must successfully implement and be adopted, so addressing these problem statements is essential. Improved security, privacy, and interoperability are just a few of the many potential advantages of implementing safe healthcare IoT using blockchain technology. Scalability, interoperability, regulation, privacy, and complexity are just a few of the issue statements that need to be addressed. More specifically, the current dearth of scalable and interoperable blockchain solutions for healthcare IoT devices, the requirement for effective regulation and privacy measures, as well as the potential complexity of blockchain technology, may obstruct the successful adoption and implementation of blockchain-based secure healthcare IoT. Addressing these problem statements will be critical for realizing the potential benefits of blockchain-based secure healthcare IoT scenarios.

1.4 Research Objectives

Objectives:

The following are the objectives of the proposed research work:

1. To Enhance the performance of IoT-Based Healthcare Monitoring System.
2. To Design QoS-Aware and Secure IoT Networks for Healthcare System.
3. To Develop Secure Data Processing Models for IoMT Network Using Blockchain.
4. To Improve Attack Detection and Resilience in IoMT Networks.

1.5 Organization of Thesis

The structure of the Thesis is organized as follows,

Chapter 1 It begins with the with an overview of IoT's role in the healthcare system, followed by discussions of its contributions to various fields of research and present applications. It also gives incentive for the research activity. The next section discusses the issues that are encountered when designing a healthcare system.

Chapter 2 Presents a comprehensive literature review on Healthcare IoT components and their features, as well as the various security approaches utilised for Healthcare IoT implementation scenarios. The Internet of Things enables remote health surveillance options. The most efficient methods for building home monitoring systems for people with chronic illnesses needed a significant amount of time and effort from patients. It also focuses on research gaps that are identified by reviewing past research papers.

Chapter 3 Presents the design of various models for deploying healthcare scenarios. To improve QoS performance in response to various types of attacks, these models employ high density feature extraction and classification approaches.

Chapter 4 Using deep learning models, improves the efficiency of IoT-based medical monitoring and control system. The system is tested against four distinct sorts of ailments, and it is determined that for each disease, the system model improves the patient's condition more quickly. However, the model can be enhanced further by testing it on a greater number of patients and doing a more in-depth analysis of system performance by taking into account a wider range of disorders.

Chapter 5 The system approach combines the interactive Q-Learning and Genetic Algorithm (GA) to incorporate QoS and security knowledge. As a result, when faced with network hazards, the model outperforms in terms of latency, energy consumption, throughput, and PDR. The model integrates the GA Model, which predicts the different sidechain configurations, with the interactive Q-Learning Method, which helps with the dynamic scaling of the underlying blockchains. Following a temporal quality of service study across many block batches, incentive functions are generated via the interactive Q-Learning Method.

Chapter 6 IoMT data processing paradigm for applications in healthcare. Since the suggested solution first maintains patient data on a single linked blockchain, it demonstrates distributed computing capabilities, transparency, traceability, and immutability.

Chapter 7 Provides the analysis of results for different evaluation parameters of three different models.

Chapter 8 Concludes the Thesis by summarizing the contributions to highlight the objectives of the research work and elaborates on future work that must be completed in order to improve the system's capabilities.

CHAPTER 2

Literature Review

2.1 Related Work

Due to Healthcare IoT expansions, it is essential to create a Wearable IoT (WIoT) ecosystem rather than only creating wearable devices, where data from body-worn sensors is synced to cloud services via the IoT infrastructure. On top of the IoT architecture, the new integrative framework for WIoT is currently being created. In the next section, we will explore the architecture of the WIoT, which is a system that would provide several advantages to the healthcare business, as well as the connections that exist between many different sections.

As a frontend component of the Internet of Things, invisible wearable body area sensors (WBAS) cover the body to collect data on the health of the person who is wearing them. The main purposes of WBAS includes: 1) using touch sensors or other peripheral sensors to collect data from the body and mistakenly record body activities; and 2) Getting ready data for remote transfer for detailed on-board analysis for close-loop feedback or analysis and decision support. Primary functions of WBAS always feature a tiny sensor, an integrated CPU with storage capabilities, power management, and occasionally even communication circuits, regardless of whether they are intended for mass production or merely research and development. One example of a wearable sensor that acts as a peripheral to a fitness tracker is the BodyMedia bracelet, which was developed by Jawbone Inc. in the United States. Its purpose is to encourage customers to lead active lifestyles with fewer hardware requirements and fewer computationally intensive algorithms. Most contact-type wearable sensors have the necessary electronics and processing power to create precise, high-resolution clinical information on patients in real time. To effectively acquire data in the realm of wearable technology, a unique interface between the body and the sensor must be developed. Modern sensor sites, such as the the ring sensors for pulse oximetry [4], chest-worn ECG monitor [5], the attachable BioPatch [6], and others, make it possible to constantly monitor vital signs. Folks may soon be able to monitor their own health by using smart textiles, which are the cutting edge of wearable electronics that are woven into the fibers of garments. This will eliminate the need for individuals to make regular trips to hospitals or physicians. It has been shown that smart clothing that integrates textile-based sensors may be beneficial for the purpose of

monitoring the reaction of the autonomic nervous system [7].

WBAS must follow worldwide quality standards regardless of the end-user applications they support to keep their ability to operate with the least level of supervision. Because of the needs for wearable sensors, electronics have been miniaturized, and effective ways for decreasing power consumption while maintaining clinically acceptable levels of performance have been developed. Both of these trends have been driven on by the demand for wearable sensors. Researchers now face difficulties processing data from wearable sensors since it needs to be accompanied by details like time, activity, and location.

WBAS are hardly ever utilized as standalone devices because of their limited processing power and bandwidth. They must therefore transfer data to more powerful computers that might be located nearby in the form of smartphones, tablets, and laptops or distantly on the cloud. In order to store and process the data that sensors collect, it is either uploaded to the cloud or routed to server centers, where it may be stored and processed. This happens in both cases. This data transmission is made possible via companion devices, which also serve as gateway devices. Wearable sensors might be able to communicate with Gateway devices by utilizing Bluetooth and other short-range communication methods. The data acquired by these sensors can subsequently be sent over to the cloud via Wi-Fi, GSM, or other heterogeneous networks. The data may be stored on the gateway device, algorithms may be used to ascertain its clinical relevance, and data may be transferred to remote servers when required. Researchers have shown that health care providers may assess the techniques used by their adolescent patients to maintain a healthy weight using information from weight scales [8]. This is accomplished by transmitting the data from the scales to a smartphone, which then uploads the data to a remote server. Smartphones and cloud servers may be able to communicate in order to track how frequently older persons trip and fall [9]. These few examples illustrate how connecting to a user's smartphone or mobile allows wearables and other devices to send data to faraway servers. The Mobile Cloud Computing (MCC) paradigm optimizes mobile computing and networking protocols to increase smartphone speed and battery life. WIoT may gain from MCC since it will open the door for cloud-based data processing and storage. This is one of the potential advantages.

The combination of mobile phones and wearable sensors cause an unparalleled flow of medical data to be produced and stored on the cloud. Studying the body is crucial, but analyzing this knowledge is as important. Patients can only benefit from wearable sensors

if sophisticated algorithms are used to evaluate the data and provide advice. A cloud computing infrastructure may make it possible to do complicated processes. In addition to making wearable data management simpler, this also includes data mining, machine learning, and medical big data analytics. The pairing of WBAS and MCC, known as the cloud-assisted BAS (CaBAS), is helping to pave the way for scalable, data-driven, and ubiquitous healthcare. The following is a list of some of the ways in which the WIoT can benefit from CaBAS: 1) routing protocols that enable handshaking and simple data transfer between wearable sensors and telephones; 2) minimising pointless data processing on wearable sensors with constrained resources using event-based processing; 3) Clinical data with activity-level annotations to increase the precision of cloud-based machine learning algorithms; and 4) cloud-based machine learning algorithms that can learn from and adapt to their surroundings.

2.2 Different use cases of Healthcare IoT

Applications that are useful in an emergency situation emergency application may be able to rapidly warn authorities of any unusual occurrences by using the Internet of Things [28]. It may be accomplished, for instance, by using medical equipment to maintain tabs on the health of a patient, followed by personal mobile devices doing an analysis of the data acquired to detect emergency conditions, and lastly by transmitting information to medical information systems. It is possible that the ambulatory team will attempt to contact the patient in the event that an urgent problem is detected. Because of this, the medical center gets ready to start the clinical therapy, and the physicians and nurses provide instructions on first aid that are particular to the situation. The authors of [29] described a healthcare system that utilised both telecare for emergencies and telemedicine diagnostics. While diagnostic telemedicine gives the user information about illnesses, medical knowledge, and alternative therapies, emergency telecare discloses the user's location, the nature of the emergency, and directions on how to help. The authors Korzun et al. offered a variety of options for using digital emergency assistance [30]. There is an urgent need for mobile applications that can detect and prevent falls due to the enormous detrimental effects that falls have on the health of the elderly. The market now offers fall detection systems in three main categories: vision-based systems, wearable sensors, and ambient sensors. A system for real-time fall detection was proposed by Cheng et al. [32] and uses wearable sensors to track the wearer's motions and positions. 15 diverse actions

in total (10 purposeful falls and 5 common place behaviours) were used to assess the suggested technique. A total of thirty repetitions were made of each exercise. The results of the testing showed that the fall detection algorithm's total accuracy was 96.4%. An alternative method for detecting falls is to use the depth sensor of the Microsoft Kinect to track the motion of both human and non-human objects in depth frames.

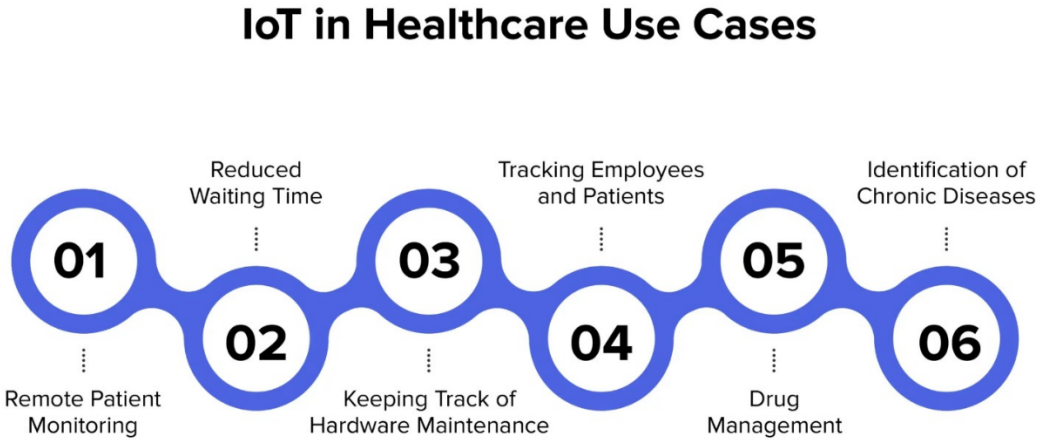


Figure 2.1 Uses Cases in IoT Healthcare.

2.3 Models used for deployment of Healthcare IoT scenarios

Modern technology, including wearables, sensors, mobile internet, cloud platforms, data analytics, and artificial intelligence, is used in "smart healthcare," a system that offers better medical care. To manage and store health records, information and communication technology is used. Access to telemedicine, telesurgery, and remote monitoring are all part of the system. It also facilitates electronic input from patients and physicians and promotes dynamic access to health information. The Internet of Things is commonly utilized to increase patient satisfaction and provide rapid, efficient care. The IoT's ability to link together previously siloed medical resources has allowed for the development of novel, trustworthy, and highly efficient healthcare services. Internet of Things (IoT) system development may range from the very simple (continuous patient health monitoring) to the extremely complex (telesurgery using surgical robots and mixed reality tools). The article [7] describes the architecture of a cheap IoT platform for health monitoring using e-health technologies. Sensing devices, such as thermometers, respirometers, and pulse monitors, keep tabs on vital signs. These sensors report their findings to a cloud-based E-health platform. The technology will automatically match patients with appropriate physicians based on their vital indicators.

A particular low-cost Internet of Things (IoT) gadget is incorporated with [8] to

concurrently monitor hospital patients and provide the data to clinicians throughout the globe. Using a Raspberry Pi and two MSP430 microcontrollers, data is gathered and delivered. The Raspberry Pi can wirelessly transfer data to any networked system due to its integrated Wi-Fi adapter. Table 1 contains a list of the data communication methods that can be used between the microcontroller and the cloud. Real-time tracking of vital indicators is done via the wristband's sensor. wirelessly transferring the MSP430's saved data to the proper medical professionals for additional treatment. Both private homes and institutional settings, like hospitals, can make use of smart healthcare. In an IoT architecture, CO2 is monitored via an Indoor Air Quality (IAQ) technique [9]. In order to ensure that healthy people and bedridden patients are not harmed by the air inside, an assessment of the air quality is performed. Here, carbon dioxide is measured using a CO2 sensor. Using a mobile device, the sensor's readings are sent to the internet for storage. When the carbon level rises over a preset threshold, the necessary personnel are notified so that they may take remedial and preventative measures, and the user is able to monitor the data on a regular basis.

Drug management is an important and necessary chore for everyone with a chronic illness or other condition. Elderly individuals, in particular, have a hard time keeping track of several medications. Unfortunately, dosage schedules are often altered or forgotten. An Internet of Things (IoT)-based medication reminder is created to help patients who have trouble remembering to take their pills on time [10]. It reminds the patient to take their medication exactly as prescribed. An Internet of Things-enabled pill box with a sensor to determine whether or not to assist patients who struggle to remember to take their medications on time, an Internet of Things (IoT)-based medication reminder is developed [10]. The patient will be reminded to take their prescription as prescribed medication was taken. Customers may rely on the system to send them timely prescription reminders. Patients and carers can both use the resulting app to access information about medications. This makes it much easier to monitor pharmaceutical supply, storage, and use. Anyone can learn about and follow their drug cycle using this method, and it won't have an impact on performance in a variety of situations.

Modern healthcare has a significant impact on the preservation and safety of soldiers operating in conflict zones. This study recommends employing an IoT system to track a soldier's health and other data in order to better comprehend their position [11]. This system includes a temperature sensor, an accelerometer, a bomb detector, an ECG module, and a GPS receiver. Based on the data obtained by these sensors and delivered

to a control unit situated in the fighting zone, wireless real-time notifications are given to authorities. The data is duplicated and kept in the cloud for future review.

The Internet of Things has the potential to improve seniors' quality of life in a variety of ways. Elderly care is a must if we wish to increase the average human lifespan. Social and individual concerns of the elderly must be taken into account while delivering healthcare. When it comes to doing daily physical activities, the elderly population need help because of their unique demands. Movement, medicine, personal care, and adequate diet are just some of the things that may help seniors maintain their health. The use of the Internet of Things helps the elderly complete their daily duties and enables their loved ones and carers to keep an eye on them at all times. It links together existing medical facilities and provides high-tech, reliable, and reasonably priced medical treatment to the public. Using IoT technology, we can keep track of how the elderly are feeling and how they are doing medically. For the purpose of keeping tabs on the elderly, the Internet of Things-based healthcare infrastructure is outfitted with sensors like those used in oxygen monitors, fall detectors, cameras, and light meters [12]. GPS technology can be used to track patients' positions in real time while sending data to the cloud. The system's sensors provide ongoing monitoring, and the data are relayed to a cloud service. After cloud-based analysis of the data that has been stored, feedback is given to the user. This makes it possible to continuously monitor patients in real-world settings, which is especially helpful for the care of older people.

Physiological or biological stress is how we experience it, as humans. This might be due to factors like an overwhelming workload, bad working circumstances, an absence of social support, health difficulties, etc. It's essential to recognise stress if you want to live a healthy life. Rising stress levels have a harmful impact on everyone's health. The Internet of Things presents several use cases from various vantage points to let a system detect this strain. A wearable sensing method including a three-axis accelerometer and an electrocardiogram (ECG) monitoring jacket was introduced in [13]. A GPS tracker might be used to find the individual in a high-stress setting. Stress levels may be measured with the use of an electrocardiogram by monitoring the heart's electrical activity. Through the use of modern tools, we may more easily track down the concerned individual, ascertain their exact whereabouts, and keep them safe from harm. In this work, we evaluate the ergonomic stress experienced by regular computer users [14]. When combined with stress from work, prolonged computer usage has been linked to both CVD and CVS. The optimal distance between the user and the computer, as well as the optimal angle at which

the screen should be positioned, are determined by an accelerometer and an ultrasonic sensor to provide a comfortable and productive work environment. Data from the pulse sensor is used to determine the work pressure. If the user's threshold is not reached, they will get a text message or email informing them to take measures. This method will assist computer users be aware of the dangers of computer-related eye strain and stress.

Life has become tougher for those who have disabilities because of the challenges they face in doing routine chores and interacting with their surroundings. Mental health issues, physical impairments, sensory impairments, difficulties with neurological function, and other causes may all contribute to these restrictions. The Internet of Things provides automated solutions that level the playing field for persons with impairments in social and professional settings. When facing a life-threatening situation, the simplest course of action is to activate an alarm or get an alert. They have a plethora of new systems in place to let them function independently of human input. The software was developed with the goal of improving HCI (human-computer interaction) (HCI). Anybody, even those who have never used a computer before, will be able to navigate this system with the help of this technology. A microcontroller with an attached accelerometer and mouse simulation is worn on the head and operated with the hands. The accelerometer measures the four possible head orientations, while the mouse emulation tracks the hand's location in space. After downloading and installing the app, users connect their computer or mobile device to the cloud. Each and every one of the person's postures and actions are tracked and recorded based on the head and hand motions. The patient's motions trigger the activation of the mouse and keyboard keys. For the fully or partly handicapped, a paper wheelchair with autonomous controls is developed [15]. This item may be affordable for even the most modest of budgets. An infrared sensor included inside the wheelchair follows the user's blinks to fine-tune its movement in any direction. This procedure is utilized to reduce the physical strain on the sufferer. The system alerts the predetermined emergency contacts via the global system for mobile communication (GSM). For less environmental impact, the 12V battery banks in this system are charged using solar photovoltaic technology.

[17] suggests that a prototype based on the Internet of Things be created to help patients who are blind or visually impaired. This device aids the blind and visually handicapped by scanning the surrounding area and sounding an alarm if it detects an obstruction in its path. The ultrasonic sensor can detect obstacles by being attached to the wearer's spectacles. The sensor is able to detect moving obstacles coming from a variety of

directions. Using the smartphone's built-in GPS, the sensor can pinpoint the user's location. Once the sensor senses an obstruction, it will alert the user. The database keeps track of where obstacles are installed, and that data is used to provide a warning to anybody traversing a selected set of coordinates.

Individuals rely on wearable technology to meet their most essential computing needs. New inventions in the digital ecosystem that aid medical diagnosis have arisen in response to recent breakthroughs in sensor manufacture, communication, and data analytics. Wearable technology has expanded beyond smartphones to hats, socks, shoes, and other articles of clothing. Many wearables can now be used without the need for individual software installations thanks to developments in cloud computing. As a result, offering the health monitoring system at a lower cost is simple. Wearable devices made possible by the Internet of Things may help everyone from healthy people to those who are paralyzed or otherwise disadvantaged monitor their health and, for example, diagnose diabetes or heart problems. A simple auto-calibration technique was used to construct the system's small device, which consists of a potentiostat and processing unit [18]. The PID sensor is useful for determining how much alcohol is currently in our systems. The gas sensing system is integrated into a wearable device. It is like a potentiostat in that it can be powered through USB, signals are sent over Bluetooth, and it has a high output. An ECG monitoring device with three leads was proposed for continuous monitoring. This gadget features sensors for monitoring purposes, and the data it collects may be sent wirelessly to a server in the cloud Data exchange in the cloud uses both the Hypertext Transfer Protocol (HTTP) and the Message Queuing Protocol (MQTT) [19]. Users can access real-time ECG data with this module from anywhere. These protocols offer quick data transmission, enabling continuous monitoring. Another method for continuous diabetes monitoring has been devised [20]. There are also additional accessories, such as necklaces and bracelets. A strain gauge for the neck, a moisture sensor, a temperature sensor, a wrist-mounted heart rate monitor, a pressure sensor, and a weight sensor are among the sensors it has that can be used to detect motion and response (socks). Machine learning methods like particle swarm optimisation are used to estimate the diabetic patient's health using the sensor data that has been gathered. Using a wearable device, a handicapped person may interact with a computer using subtle movements, such as a nod of the head or a blink of the eye [21]. The system tracks the position and motion of various body parts using an accelerometer sensor and an infrared (IR) sensor connected to a computer. This allows the pointer to roam freely across the screen in a variety of ways.

2.4 Security models used for Healthcare IoT deployments

Because to IoT integration, many new insights have been acquired, productivity has grown, and expenses have decreased, all of which have helped to improve people's quality of life generally. IoT is being utilized in healthcare to improve patient monitoring, save costs, and stimulate innovative treatment philosophies. In contrast to the "industry 4.0" trend of integrating IoT technology into production and retail, "Medicine 4.0" and "Health 2.0" are spreading quickly in the industry of healthcare. New methods for asset management, remote monitoring, autonomous assistive devices, medication administration, proactive treatment plans and early warning systems, and equipment maintenance has been carried out consequently. One of the Internet of Things' (IoT) most important uses in healthcare is remote patient monitoring. This application has the potential to save millions of lives and a significant amount of money, even though other areas of healthcare are still absolutely necessary. For a variety of healthcare applications, wireless body sensor networks (WBSN) have emerged as a crucial Internet of Things (IoT) platform. Qadri et al. [1] provide a thorough explanation of the usage of wearables to evaluate fitness and health in HIoT in their article. The Internet of Things, however, has a lot of potential in the medical field and could be helpful for early detection, diagnosis, and treatment. The Internet of Things (IoT) for medical device integration is now focusing on consumer endpoints, such as Continuous Glucose Monitoring (SGM), blood pressure cuffs, ingestible sensors, connected inhalers, and other gadgets made to gather data on patients' vital signs. Another device of this kind with detectors for Parkinson's disease symptoms was just released, and its name is Apple Watch. Patients getting WBAN have sensors and actuators attached to their bodies in a variety of methods, each of which is intended to fulfil the precise information needs of the medical team and the particular medical condition being treated. In the medical profession, this entails that data may be gathered automatically and that decision support criteria may be used, enabling the administration of prompter treatment. HIoT systems must have the necessary security and privacy measures to ensure patient confidentiality, efficient care delivery, and patient safety. But the healthcare sector is where security and privacy vulnerabilities tend to manifest themselves first and primarily [2]. Medical data is seriously at danger from malware, financial human manipulation, and the loss of personally identifiable information. Many of the most advanced Internet of Things technologies now accessible are notably deficient in the security and privacy pillars. As a consequence, there are

significant privacy and security risks with very sensitive data. By the end of 2019, 84% of security breaches will be tied to the Internet of Things, predicts a poll conducted by the research firm Aruba [2]. IoT devices frequently have low power requirements, constrained processing and storage capacities, and subpar user interfaces. These factors all add to total complexity and tempt developers to overlook IoT security. To enable secure data transfer, sharing, and use, make security the procedure's cornerstone. A modern approach is required to efficiently use this technology while protecting people's privacy [3]. There are several potential applications for technologies like nanotechnology, blockchain, big data analytics, edge computing, biometrics, and machine learning outside of the conventional sectors for which they were first created. Instead, these advancements might be included in a range of approaches, like those meant to guarantee the privacy and security of IoT gadgets. The authors of this study examine various strategies, frameworks, and practices for safeguarding user privacy in the IoT. The majority of papers on the HIoT explore the aforementioned new technologies and potential applications for them in the context of remote patient monitoring because of how versatile the device is. The authors also discuss potential future paths for creating original and secure solutions for applications like HIoT.

The UK's Information Commissioners Office (ICO) claims that the healthcare sector has an inordinate number of data breaches. The ICO has collected a comprehensive list of data breaches in the healthcare industry. Sensitive personal data handled by the healthcare business includes static and dynamic behavioral data collected by sensors and giving insight into an individual's private life. This data may include both moving and static components. Due to the risk that the exposed data poses to users, this constitutes a very serious data security violation. The breakdown of the various privacy protections that can be utilized by any and all horizontal layers of an IoT architecture is provided in Table IV. Due to their processing power and power, it will probably be challenging to guarantee security and privacy when the objects layer or sensor devices are involved. Explicit identifiers, quasi-identifiers, and privacy features make up the three primary groups of sensitive healthcare data. Personal information in a patient's medical record is identified using explicit identifiers. Such data includes things like the patient's name, any identification or serial numbers, and their contact information. Age, ZIP code, and birthdate are a few examples of "quasi-identifiers," or traits that can be used to approximatively estimate other forms of identification. Information concerning a person's income, health, or disability is an example of private information that should be protected.

The kinds of data that are covered include tax returns and medical records. Methods based on random perturbation and data anonymity, such as k-anonymity, l-diversity, and confidence bounds, are generally used to address these kinds of problems. However, with regard to classified material, traditional anonymity is not applicable. Since hackers can utilise background knowledge attacks to locate data connected to certain use cases, this absence of restrictions may result in privacy violations under real-time use cases.

Despite their importance, the risks that the Internet of Things poses to consumers' safety and privacy are often disregarded. The authors of this study review the body of knowledge on HIoT security and privacy as well as the tactics used to promote the broad usage of cutting-edge solutions that ensure the protection of sensitive data. The Authors also take into account methods for promoting the widespread use of cutting-edge technology that ensure the protection of sensitive data. Wazid et al. [11] look into user authentication and safe key management techniques for a scenario including fog computing and the Internet of Things (IoT). Both a user authentication method and a key management system with three levels of verification are included in the SAKA-FC security system. Together, these two elements help to provide security. By employing a paired secret key management technique, we manage keys by creating encrypted connections between IoT devices and fog servers as well as between fog servers and cloud servers. The key management process could be kept secure as a result. It utilizes a number of authentication methods, including as passwords, fingerprints, and the user's smartphone, to safeguard the security of the user's data. In order to protect connections between users and IoT devices when a user has successfully registered a device, the process's next step necessitates the creation and use of a session key based on mutual authentication. For Internet of Things devices, SAKA-FC employs bitwise XOR computations, a trustworthy one-way cryptographic hash function. Elliptic curve point multiplication and a biometrics fuzzy extractor technique are used by users and fog servers, respectively.

The SAKA-FC system takes the CK Advisory model into account in addition to the DY model. The authors assert that the SAKA-FC session key-based method provides a greater level of security than the formal method that makes use of the AVISPA tool [11]. The SAKAFC, they continue, makes it hard to guess a user, a fog server, a smart device, or even an offline system. As a result, it might be safe from attacks like replay and man-in-the-middle. It also protects your privacy by obscuring your identity and making it more difficult for outsiders to observe the specifics of your discussions (ESL). The study on the safety of implanted medical devices (IMDs), such as pacemakers and insulin pumps, has

been evaluated by Wazid et al. For implanted medical devices (IMDs), the authors of this work offer a simple, three-factor remote user authentication method based on elliptic curve cryptography (ECC). The Dolev-Yao threat model, a system model connected to the IMD, the Controller Node (CN), and the User (CN), is used to illustrate the recommended security strategy. The recommended approach might be strengthened by adding three-factor authentication for remote monitoring and paired key configuration between CN and IMD [12]. Challa et al. [13] and [14] carried out two other crucial investigations, and they also propose a biometric-based three-factor authentication method for cloud-assisted CPS installations in addition to a similar security method for wireless healthcare sensor networks. [13] and [14] Despite this, the employment of the fog server model or device model for the anonymity and privacy of the user data was not discussed in the study [12][13]. Wazid et al. offer their Lightweight Authentication Method for the Cloud Internet of Things in a different publication [15]. (LAM-CIoT). This approach combines bitwise XOR operations with one-way cryptographic hashing. Moreover, a fuzzy extractor. Additionally, local biometric verification is carried out utilising a fuzzy extractor method at the user's end. The seven-step process that verifies the user's identification uses three distinct components. 1) Even though it comes in second place after the password, the user's electronic identity card—which contains details about their biometric traits—is just as important. By employing a timestamp and synchronizing all of the clocks in the application environment, the approach keeps its anonymity and untrace ability. For mobile health applications, Yang et al. [16] present the lightweight data transfer technique with traceability (LiST). This system paradigm incorporates the Key Generation Centre (KGC), a well-known organization that gives data users access to secret keys while setting public parameters for the entire system. WBSN, the data owner, and healthcare professionals, who are the data users, are also considered in this strategy. Additionally, the system has a public cloud. This system successfully integrates user revocation, traitor tracking, and granular data access via keyword search across encrypted EHR with an encryption approach. The authors claim that LiST provides lightweight features like lightweight traitor tracking, lightweight decryption and verification, lightweight user revocation, and a lightweight test method [16]. To safeguard the privacy of electronic health records, this technique eliminates unauthorised users and users with decryption privileges by utilising a bare-bones revocation process. On top of Software Defined Networks (SDNs), Meng et al.'s [9] security architecture for hospital networks is constructed. The need for specific device settings is eliminated by software-defined

networking (SDN), which separates network policies from networking hardware. Software-defined networking (SDN), according to the authors, protects wireless medical sensor networks from a variety of threats, including denial-of-service and flooding attacks, in the context of cybersecurity and healthcare. According to the study's conclusions, the optimal course of action for identifying the status of packets and the profiles of connected devices is to create a trust-based SDN solution for WMSN that is based on Bayesian inference. The authors' method seems to be one that can successfully detect fake hardware in a range of deployment scenarios while also being scalable, according to the study's results. The authors advise doing further study on the topic so that the effectiveness may be assessed from a more comprehensive angle. In their paper [17], Porambage and colleagues provide a privacy framework for Internet of Things (IoT) systems, along with the requirements for setting one up and potential challenges. The authors stress the significance of enforcing traditional and sophisticated privacy laws thoroughly in light of the abundance of IoT devices. Despite the availability of simple privacy settings, Porambage et al. claim that these options are not secure because it is simple for attackers to monitor them. Customers may have privacy concerns if internet service providers (ISPs) and cloud service providers (CSPs) are used together for the transfer and storage of user data, according to the authors. The Health Internet of Things (HIoT) relies heavily on remote health monitoring because user data is readily available. This has made privacy concerns about users and patients more visible, and stronger privacy frameworks are required to ensure users' and patients' safety. Alternative privacy-enhancing technologies (PETs) abound, but scenario-based PETs and the technology that supports them are far more often utilized in the context of WSN. By using cryptography-based privacy solutions, wireless sensor networks (WSNs) are safeguarded against both internal and external privacy assaults. Complex cryptographic algorithms may make it more difficult for WSNs to successfully manage the resources and energy that have been provided to them, even while computationally intensive attacks may succeed. The PETs are therefore in need of additional solutions that may be modified to suit the requirements of each individual IoT application. Additionally, the authors [17] include "proxy as a broker" and "privacy coach" as two examples of privacy-improving technologies that permit the scalability and interoperability of IoT systems. The details of each of these strategies are provided here. The same degree of location and identity security may be offered by employing public key cryptography together with a forwarding agent. PbD is a well-known privacy solution, and [17] makes the novel suggestion that it be employed

in IoT networks. Because it utilizes big data analytics, cloud computing, legal frameworks, and sensing technologies, this strategy is among the most popular ones. It guarantees the solution's privacy from the very beginning of the design phase and throughout the entire process. Large volumes of medical data can be handled privately using the method described by Yang et al., who also describe how to store the data so that it can be continuously updated [18]. This system's three primary features are intelligent deduplication, self-adaptive access control in both routine and emergency scenarios, and cross-domain data interchange. Compared to other privacy-preserving techniques, this one works better. The authors of the study give a summary of the numerous components of this methodology. The features include password-protected Break Glass Keys (BGK), cross-domain Break Glass Access (BGA), and attribute-based encryption. This innovative solution enables cross-hospital data transmission utilising a cross-domain approach, quick and easy emergency access to encrypted data, and cross-hospital data access using BGA and BGK approaches. In this research, we propose a method for safeguarding user privacy by applying the BGK methodology. The BGK method is protected with a password, offering an additional layer of security. A three-factor authentication method utilising biometrics, smartcards, and mobile authentication was a suitable solution to the security issues in the traditional password-based verification, according to the aforementioned study. [11][12][13][15][14]. Previous studies didn't offer any comprehensive remedies. IoT applications for health-related purposes produce a lot of data, which is first processed locally on the device before being transferred, saved, assessed, and fed back into the applications to help with better decision-making. The aforementioned presentations [16–23] as well as the in-depth analysis [1] by Quadri et al. make it abundantly clear that IoT application security and privacy were disregarded, that solutions had flaws, and that there was no reliable security recommendation for healthcare IoT spectrum sets.

2.5 QoS aware models used for Healthcare IoT deployments

The sorts of emergency biometric data that may be gathered by a WBAN system, which generally comprises of a large number of low-power sensors, include data from electroencephalograms (EEG) and electrocardiograms (ECG). Data from several kinds of biometric sensors are among the emergency biometric data that a WBAN system may gather. When these insightful biological data are originally gathered, The patient might, for instance, keep track of their own health in real-time using an on-body gadget (the target hub). The target hub then sends these settings over a wireless network or the

Internet to distant off-body devices (such a central monitor). The doctor will be able to choose the most effective course of treatment once they have correctly diagnosed the patient's condition. Compared to wireless communications that occur over the air, which do not have to deal with live tissues as their transmission channel, implanted medical devices have a variety of challenges. High-frequency electromagnetic radiation encounters resistance in the human body, preventing signal transmission. This is the first issue. Due to the intrusive nature of implantation operations, the devices that are implanted must adhere to strict miniaturisation and service delivery standards. The most difficult task is without a doubt figuring out the best technique to provide Quality of Service (QoS) for medical applications [5]. There is no way to rule out the possibility that the implant WBAN supports the transmission of a variety of medical data kinds, including at least some non-emergency and some emergent data types. Even while it's important to arrange the data on medical disorders that don't need urgent treatment to meet the needs of certain applications, it should never lose its top priority status (HP). The Pill Cam implant may capture video of the digestive tract, replete with base layer and enhancement layer data streams, when used in conjunction with a camera. Then, this data might be examined. Emerging data is reflected in the enhancement layer for low-priority (LP) data and the foundation layer for high-priority (HP) data, respectively. Non-emergent data are not reflected in the base layer. Because there are so many competing performance expectations, different priority levels must be used when transmitting medical data. Medical information from other implanted devices, such as oximeters, deep brain activity sensors, pH, glucose, and intracranial pressure monitors, should be sent in addition to the data from the Pill Cam. Because of the integration of collaborative technologies, the implant WBAN now provides a selection of quality-of-service (QoS) options and can transmit medical data with high levels of dependability [6, 7]. The traditional cooperative implant WBAN configuration that is shown has been the focus of several studies. A common use case for the decode-and-forward (DF) and amplify-and-forward (AF) relaying protocols is data transmission between an off-body access point and an implanted device (source). The letters DF and AF stand for "decode and forward" and "amplify and forward," respectively (destination). To put it simply, the DF technique's relay enhances the received signal before relaying it. However, in the AF approach, the relay first extracts the source information from the incoming signal before re-encoding it and only then transmitting the information. However, DF and AF techniques are ineffective because the collaborative WBAN is constrained by the connection that has the weakest component channel out of all of them. The implant WBAN system is expected to perform better than the traditional cooperative WBAN in this situation, and the problem may be overcome. This is made feasible by the implant WBAN system's ability to choose the transmission

nodes depending on the strength of the channel connection opportunistically [8]. Opportunistic scheduling requires buffers at the relays in order to work effectively [9]. Incoming data is temporarily stored in the buffers until a channel quality suitable for transmission is found. Relays in implanted WBANs may soon be able to include both a sizeable and a small buffer due to advancements in modern data storage technology. There will be greater freedom as a result. Even though this approach has several real-world limitations [10], adding buffer-aided relaying may considerably improve WBAN performance. [10] (such as by creating latency or by making the relays more complex) (such as by introducing delay or by making the relays more difficult). Hierarchical modulation may be utilized to provide a variety of options for quality of service [11], and this fact has been well reported. The bitstream can be broken into multiplexed sub-streams with varying priorities (such as HP and LP sub-streams) using hierarchical modulation. Therefore, from the perspective of the physical layer, it is reasonable to predict that hierarchical modulation may be employed to satisfy a variety of quality-of-service requirements for implant WBAN.

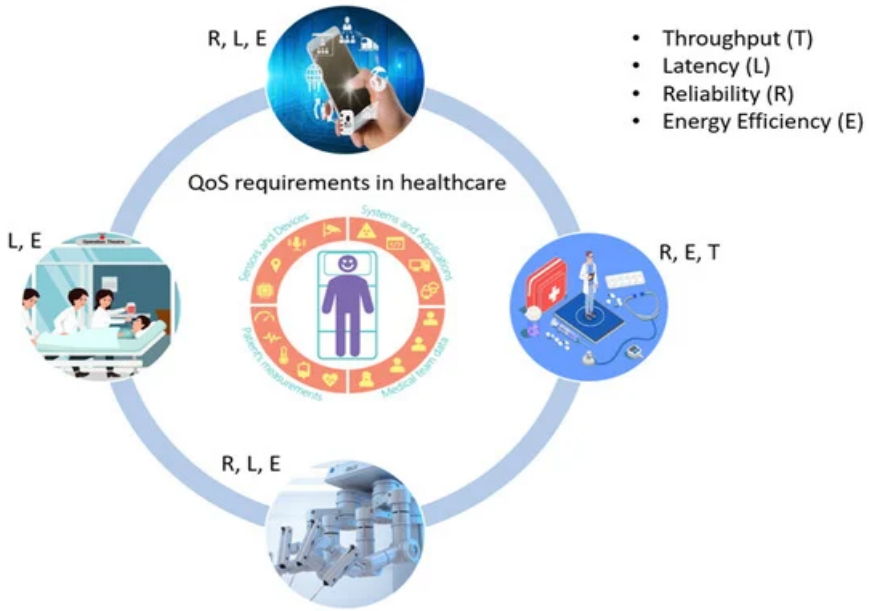


Figure 2.2 QoS Monitoring in IoT Edge Devices Driven Healthcare

Furthermore, even if buffer-aided relaying is inadequate for the transmission of time-critical information via the implant WBAN, hierarchical modulation may still be able to reduce the additional latency. This is so because hierarchical modulation builds signals using several levels of information. When using hierarchical modulation symbols, it is possible to minimize latency by mapping data that can withstand delays

to the lower-priority LP layer and data that is more sensitive to delays to the higher-priority HP layer.

Table 2.1 Summary of Literature Survey

S No	Author (s) / Year	Title	Name of Journal	Source / Publisher	Findings /Relevance	Research Gap
1.	Mahmoud M. Badawy , Zainab H. Ali 1 ,Hesham A. Ali ,2019	QoS provisioning framework for service-oriented internet of things (IoT)	The Journal of Networks, Software Tools and Application	Springer Nature	1.This paper presents to optimize service quality by balancing reliability and computational cost. 2.To improve performance metrics such as reliability, scalability, and response time.	1.Research gap includes effectively balance service reliability and computational cost 2.Further research is needed to explore the scalability of the QoPF framework
2.	J. Ren, J. Li, H. Liu and T. Qin	Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT	Tsinghua Science and Technology, vol. 27, no. 4, pp. 760-776, Aug. 2022	Tsinghua University Press	1. Blockchain sharding reduces system time latency by dividing consensus peers into sub-blockchains, improving time efficiency	1. Research gaps include blockchain sharding methods are primarily designed for currency applications and may not directly apply to healthcare IoT networks
3.	Nikita Malik and Sanjay Kumar Malik	Using IoT and Semantic Web Technologies for Healthcare and Medical Sector	Ontology-Based Information Retrieval for Healthcare Systems, (91–116) © 2020	Scrivener Publishing LLC	To do Remote monitoring, enhancing patient care	Further investigation is needed to enhance data security and privacy measures in IoT platforms to protect sensitive healthcare information.

4.	D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne	BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain	IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11743-11757, 15 July 2021	IEEE	This research introduces BEdgeHealth, a decentralized architecture for edge-based IoMT networks using blockchain.	Research gaps include assessing the scalability and security aspects of BEdgeHealth in real IoMT deployments.
5.	P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi and N. Kumar	BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications	IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1242-1255, 1 April-June 2021	IEEE	The paper presents BinDaaS, a blockchain-based deep-learning as-a-service platform for Healthcare 4.0 applications.	Further research could focus on the scalability and practicality of deploying BinDaaS in real healthcare scenarios.
6.	B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty	Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control	IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11717-11731, 15 July 2021	IEEE	The paper introduces Fortified-Chain, a blockchain-based framework for secure and privacy-assured Internet of Medical Things with effective access control.	Research gaps include evaluating the effectiveness and scalability of Fortified-Chain in healthcare IoT scenarios.
7.	Gioele Bigini And Emanuele Lattanzi	Toward the InterPlanetary Health Layer for the Internet of Medical Things With Distributed Ledgers and Storage	IEEE Access, VOLUME 10, 2022	IEEE	The concept of an InterPlanetary Health Layer aims to leverage DLTs and distributed storages to enhance the security and efficiency of medical data management within the IoMT ecosystem	Research gap includes to modify the architecture to enable the usage of IoMT data with machine learning applications.
8.	Shihao Xu, Haocong Rao	Attention-Based Multilevel Co-Occurrence Graph Convolutional LSTM for 3-D Action Recognition	IEEE Internet of Things Journal,vol. 8, Issue: 21, 01 November 2021	IEEE	he proposed model, AMCGC-LSTM, incorporates Multilevel Co-Occurrence Graph Convolutional LSTM and Self-Attention modules.	Further research in developing more advanced and robust DNN-based models, exploring efficient approaches for different for improved performance.
9.	Wenlong Ning, Shuhua L	Automatic Detection of Congestive	IEEE Internet of Things	IEEE	The study proposed a hybrid deep learning	Research gap need to focus on validation of a

		Heart Failure Based on a Hybrid Deep Learning Algorithm in the Internet of Medical Things	Journal		algorithm, specifically a CNN model, for CHF detection.	larger sample set to enhance the robustness of the model.
10.	Y. K. Saheed and M. O. Arowolo	Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms	IEEE Access	IEEE	The paper mentions that the future work will focus on evaluating the effectiveness of the proposed system for detecting IoMT attacks using blockchain technology	There is a gap in the existing literature in terms of security concerns in healthcare data and the interconnected medical devices in the IoMT.
11.	A. Kumar, R. Krishna murthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain	A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes	IEEE Access, vol. 8, pp. 118433-118471, 2020	IEEE	The paper presents a design and simulation of a Smart Healthcare system based on Healthcare 4.0 processes.	The research gaps related to the scalability and real-world implementation challenges of Healthcare 4.0 processes need further exploration.
12.	P. P. Ray, D. Dash, K. Salah and N. Kumar	Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases	IEEE Systems Journal, vol. 15, no. 1, pp. 85-94, March 2021	IEEE	The paper explores the application of blockchain in IoT-based healthcare, discussing its background, consensus mechanisms, platforms, and use cases.	Further investigation is required into the scalability and security issues of blockchain in IoT-based healthcare systems.
13.	S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar and R. A. Khan	A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges	IEEE Access, vol. 9, pp. 84666-84687, 2021	IEEE	This paper systematically analyzes the integration of blockchain in the healthcare domain, highlighting its scope and challenges.	Additional research on addressing the identified challenges in blockchain integration in healthcare is required.
14.	M. Zarour et al.	Evaluating the Impact of Blockchain Models for Secure and	IEEE Access, vol. 8, pp. 157959-157973,	IEEE	The research evaluates the impact of different blockchain models on the	Further investigation is needed to assess the scalability and adoption of

		Trustworthy Electronic Healthcare Records	2020		security and trustworthiness of electronic healthcare records.	blockchain for healthcare records on a broader scale.
15.	A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid and M. F. Yusof	Scalability Challenges in Healthcare Blockchain System—A Systematic Review	IEEE Access, vol. 8, pp. 23663-23673, 2020	IEEE	The paper presents a systematic review of scalability challenges in healthcare blockchain systems.	More research is required to address the scalability issues identified and propose scalable solutions.
16.	I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob and M. Omar	Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts	IEEE Access, vol. 9, pp. 37397-37409, 2021	IEEE	The paper explores the automation of procurement contracts in the healthcare supply chain using blockchain smart contracts.	Further research could focus on the practical implementation and scalability of such automated contracts.
17.	Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi	Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System	IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1877-1890, December 2021	IEEE/CAA	The paper presents a blockchain-assisted encryption system for secure healthcare data in a cloud-based cyber-physical system.	Research gaps include evaluating the performance and robustness of the proposed encryption scheme.
18.	M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman	Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract	IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10117-10130, 15 June 2021	IEEE	The paper discusses optimal witnessing of healthcare IoT data using blockchain logging contracts.	Research gaps include the practical deployment and efficiency evaluation of the proposed logging contract system.
19.	D. Lee and M. Song	MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address	IEEE Access, vol. 9, pp. 158122-158139, 2021	IEEE	The paper introduces MEXchange, a privacy-preserving blockchain-based framework for health information exchange.	Research gaps include assessing the privacy and security guarantees of MEXchange in real-world healthcare information exchange scenarios.
20.	G. S. Aujla and A. Jindal	A Decoupled Blockchain Approach for	IEEE Journal on Selected Areas in	IEEE	This paper proposes a decoupled	Further research could focus on the performance

		Edge-Envisioned IoT-Based Healthcare Monitoring	Communications, vol. 39, no. 2, pp. 491-499, Feb. 2021		blockchain approach for edge-envisaged IoT-based healthcare monitoring.	optimization and real-world deployment of the proposed approach.

2.6 Research Gaps

Despite the potential advantages of secure healthcare IoT, many research gaps remain that must be filled in order to fully realise its potential. According to the review, some of the current research gaps include,

1. **Standardization:** Secure healthcare IoT is not standardized, which might make it challenging to compare and rank various systems and devices. To create global standards and guidelines for secure IoT in healthcare, more study is required.
2. **Security and privacy:** Despite the fact that security and privacy are acknowledged as significant obstacles in secure healthcare IoT, there is still much to be discovered about how to successfully handle these problems. To provide efficient security and privacy controls for IoT systems and devices used in healthcare, more research is required.
3. **Interoperability:** More study is required to determine how to make sure that various IoT systems and devices can operate together in healthcare settings without any issues.
4. **Usability:** Healthcare IoT devices and systems must be easy to use and understand in order to be adopted by healthcare providers and patients. More research is needed to understand how to design and implement user-friendly healthcare IoT devices and systems.
5. **Cost-effectiveness:** Although secure healthcare IoT has the potential to lower healthcare costs, more research is still required to determine which devices and systems are the most cost-effective.
6. **Ethical considerations**: The use of secure healthcare IoT raises important ethical considerations around issues such as patient consent, data ownership, and algorithmic bias. More research is needed to understand and address these ethical considerations.

Overall, addressing these research gaps will be critical for the successful implementation and adoption of secure healthcare IoT deployment scenarios.

CHAPTER 3

Different Models for Deploying Healthcare Scenarios

3.1 Review of Models used for deploying Healthcare IoT scenarios

Over the years, a large number of extremely complex architectures have been put forth by researchers to increase the efficacy of Internet of Things-based medical devices for monitoring and control. For instance, the research in [3, Ch. 1] suggests using various AI-based models to measure illnesses including diabetes, mental state, Parkinson's disease, nausea, etc. In a model for monitoring these conditions using an internet of things (IoT)-based setup that is mentioned in [3, Ch. 2], electrocardiography (ECG) for the heart, electroencephalography (EEG) for the brain, electromyography (EMG) for the muscles, capnograph sensors for measuring body gases, and temperature sensors are combined to evaluate the condition of the entire body. Body & environment conditions like stress, heartbeat tracking, muscle stress levels, bed temperature, room temperature, oxygen levels, etc. are monitored and controlled via this scheme, and a k-Nearest Neighbour (kNN) classifier is used to improve the classification accuracy. For increased processing and assessment efficiency, all of this data can be further processed on the cloud. In order to transport high-speed data from IoT devices to the cloud for real-time processing, the work in [3, Ch. 3] suggests a fog-based real-time analytics solution. Cloud computing models like Amazon Web Services, Google Cloud, and Microsoft Azure monitor, process, and manage this data to deliver high-speed, low-error, and high-efficiency cloud calculations. But this data is not always secure, and needs algorithms like encryption, hashing, and hierarchical processing to improve its security. Work in [3, Ch. 7] proposes a framework for improving this security using a hierarchical & layered framework which defeats attacks like authentication, tampering, non-repudiation, confidentiality, denial of service, and authorization. These attacks are removed via standard tools, and their applications at specific system end points. Algorithms like fuzzy C-Means [4, Ch. 6] are also used for effective data clustering, wherein complex diseases like Alzheimer’s can be detected via fusion of different sensory data inputs. Evaluation of these diseases requires a large number of sensor specific data to be used in tandem with patient historical health data for improved classification efficiency. Other techniques like Genetic Algorithms (GA), Logistical Regression (LR), semi-supervised learning (SSL), principal component

analysis (PCA), support vector machines (SVM) and random forest (RF) classification models as applied to IoT-based healthcare are discussed in [4, Ch. 7]. These models are applied to heart disease detection, Parkinson's detection and Alzheimer detection using a multitude of healthcare-based sensors.

The study in [4, Ch. 8] recommends utilising three filters: the average trimmed filter, the patch otherwise average trimmed filter, and the probabilistic decision based average trimmed filter. A crucial issue when getting data from medical equipment is noise removal. The probabilistic decision-based average trimmed filter outperforms conventional filters in terms of peak signal to noise ratio values and least average error and may therefore be employed for real-time processing. Combining these filters with machine learning models like those outlined in [5, Ch. 5] can significantly increase the overall system efficiency for disease classification. This work proposes development of an arrhythmia monitoring system via combination of denoising and random forest classification models. This combination allows for an accuracy of 96% across 16 different arrhythmia classes, which is a very high accuracy considering the sheer number of classes that are being analyzed. These categories consist of Normal, Old Anterior Myocardial Infarction, Sinus Tachycardia, Ventricular Premature Contraction (PVC), Left and Right Bundle Branch Blocks, First Degree Atrioventricular Block, Sinus Bradycardia, and Ventricular Premature Contraction (LBBB). Old inferior myocardial infarction, second- or third-degree AV block, supraventricular premature contraction, and hypertrophy of the left ventricle, Heart artery disease and atrial fibrillation or flutter are ischemic alterations. Due to the sampling-based filtering method, an accuracy improvement of 20% is achieved. IoT based healthcare devices can also be used for monitoring remote patients, the work in [5, Ch. 11] proposes the design of such an IoT enabled healthcare monitoring system for malnutrition detection. Here a combination of WiFi, Global system for mobile (GSM), Bluetooth and local storage is done in order to monitor and trace remote healthcare data. This device has been used to perform tests like lipid profile, comprehensive metabolic panel (CMP), complete blood count (CBC), albumin, and total protein testing. These devices can be enriched via use of decision support systems, like Tabu search, Hyper-heuristic models, exact models, simulated annealing, and hybrid simulated annealing as suggested in [6, Ch. 7], wherein it is observed that the hybrid simulated annealing reduces costs of data processing and improves accuracy of processing by 20% when compared to simulated annealing models. Applications like detection of cancerous squamous cells [6, Ch. 13], automizing pill dispensing [6, Ch. 14],

social monitoring [6, Ch. 15] and continuous monitoring [6, Ch. 16] are possible due to the advancements in healthcare IoT technology. These advancements and their effects to highly populated countries like India can be observed from [7], wherein various IoT issues, and their improved performance has been discussed. This improved performance is in terms of speed, quality of sensing, accuracy of storage, etc. and has helped India to fight the CoVID pandemic. Other applications like non-intrusive muscular monitoring, context-aware body monitoring, diabetes management, etc. can be observed from [8], which have assisted different kind of healthcare IoT systems to improve their performance.

3.2 Healthcare IoT for improving performance.

Performance of these IoT devices can be improved via the use of edge-based processing, as discussed in [9] and [10], wherein ease of application of machine learning models along with big-data, blockchain and other high performance IoT technologies have been discussed. These technologies work on improving security, performance, and overall ease of use for IoT based systems. Extension of IoT can be done via the use of semantic web technologies like ontological mapping, resource description & web ontology language (OWL) based processing, etc. This processing assists in improving search capabilities of IoT systems, which is helpful for both Doctors, Patients, and other medical healthcare personnel. This model is shown in figure 3.1, and works in the following manner,

- Data is captured with the help of sensors, mobile devices, remote health monitoring devices, etc. and is given to semantic web servers.
- Over here, semantic information is associated with this data, and it is stored into data repositories.
- Medical centres and other healthcare professional platforms combine this data and apply data processing algorithms on these datasets for improving their processing efficiency.

  Extension of IoT systems can be done for analysis of complex human body conditions like kidney diseases. The work in [12] proposes use of logistic regression (LR) in combination with Adaptive Moment Estimation & adaptive learning rate optimization for improving efficiency of chronic kidney disease (CKD) prediction.

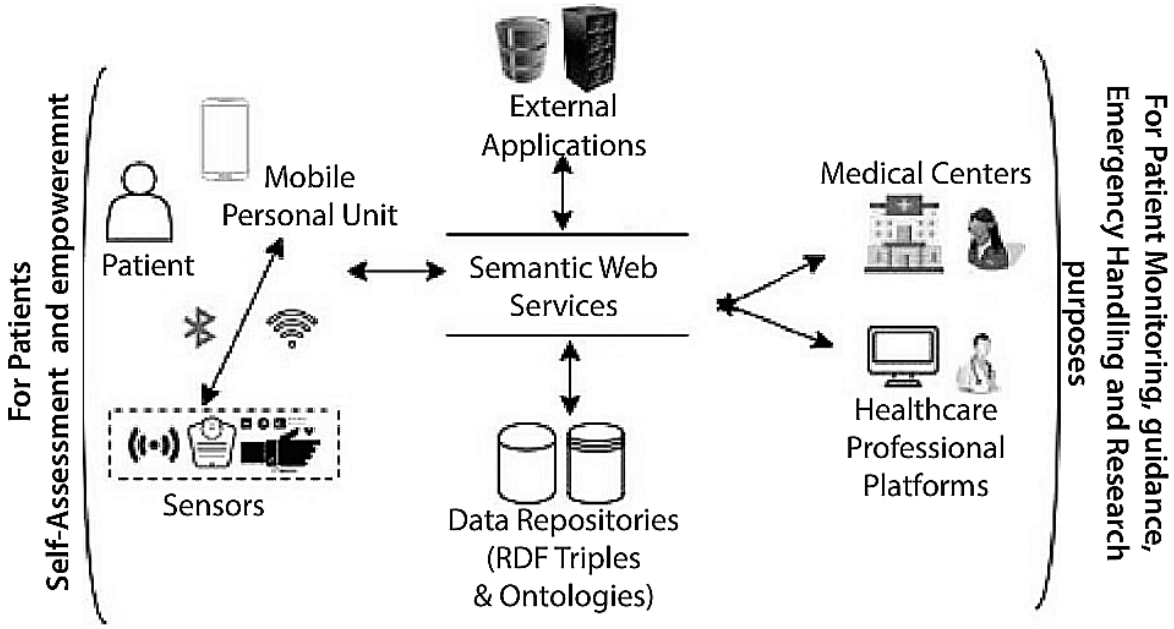


Figure 3.1. Combination of IoT with semantics for improved performance [11]

Parameters like Blood pressure, Albumin, Red blood cells, Pus cell clumps, Blood glucose random, Serum creatinine, Potassium, Packed cell volume, Red blood cell count, Diabetes mellitus, Appetite, Anemia, Specific gravity, Sugar, Pus cell, Bacteria, Blood urea, Sodium, Haemoglobin, White blood cell count, Hypertension, Coronary artery disease and Pedal oedema are used for detection of chronic kidney diseases. An accuracy of 97.5% is achieved va the use of logistic regression (LR) with adaptive learning rate optimization and adaptive moment estimation. A large number of other IoT use cases are presented in [12], wherein applications like heart monitoring, brain monitoring, muscle, monitoring, etc. are defined. Security constraints of these applications like communication issues, mobile application security issues, data integrity issues, audit log security, cloud security, etc. are discussed. If these security concerns are not effectively addressed, threats such as access to private and sensitive data, data exposure, service outages, and loss of data integrity may be introduced. The IoT network uses blockchain and other high security methods to lessen the impact of these problems. An illustration of such high security models may be seen in [14], which uses safe user sign-in authentication based on Chebyshev Chaotic-Map single-user sign-in, serves as an example of such high security architectures. This model uses a difficult set of equations to distribute authorisation tokens among IoT nodes. Each token contains data for authentication, access control, and token lifetime. These tokens are processed using the Chebyshev Chaotic-Map processor, which carries out the procedures of token reading, parsing, and

rule application.

Due to addition of complex security frameworks, overall quality of service (QoS) of these IoT devices is reduced. A backtracking search optimisation technique (BSOA) is suggested in [15] to enhance this QoS performance. This algorithm tries to improve QoS by maintaining a balance between cost of computation delay and service reliability. Flow of this algorithm can be observed from figure 3.1, and works using the following steps,

- Data is collected via a data collector entity, which monitors different data sources like sensors, datasets, environmental conditions, etc.
- The collected data is given to a data queue, wherein temporal information about this data is stored.
- Digital signal processing algorithms are applied on this data for decision making and control purposes.
- The data is then given to a service state determination unit, wherein each processing task is divided into states like,
    - Initialization state
    - Pre-processing state
    - Feature extraction stage
    - Feature selection stage
    - Classification stage
    - Post processing stage
- Data from all these stages is then combined, and a final decision is taken about the patient parameters.
- Depending upon the following parameters, the QoS parameters are then optimized,
    - Accuracy of decision making.
    - Time needed to make that decision.
    - Number of parameters considered while making the decision.
    - Number of repetitive operations performed while making the decision.
- Using these parameters, and by incorporating a machine learning optimization model, a balance between delay and performance is achieved. This balance allows the system to perform at high speed with minimum error and maximum efficiency.

Using the Analytic Hierarchy Process and Technique for Order Preference by Similarity to Ideal Solution, [16] suggests yet another such method. These models utilize the

mentioned parameters and try to select the best use-case scenarios for improving QoS of healthcare systems. The use-case scenarios are considered based on number of sensors, computational resources available and the communication overheads in the system. The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) and the Analytic Hierarchy method (AHP) are combined in the following procedure,

Evaluation of eigen values and consistency ratio is done based on the input quality metrics like accuracy, delay, precision, recall, etc. via TOPSIS.

- All these values are also given to AHP to form a decision matrix, and normalized decision matrix.
- Weights of this metric are normalized using eigen values and consistency ration values.
- Determination of positive, negative and ideal solution is done using this decision matrix.
- Evaluation of separation as a measure of alternativeness is done.
- Evaluation of closeness coefficient is done to evaluate each alternative according to their performance.
- Each alternative is ranked, and the highest rank alternative is used for final processing.

  Due to combination of TOPSIS with AHP, an improvement of 30% is obtained in the overall score values. These systems can be applied to mobile IoT systems like the ones mentioned in [16] for improved overall performance. Moreover, addition of fog assisted computing to IoT devices can also improve computation and result-evaluation performance in the system. A fog assisted computing architecture can be observed from [17], wherein fuzzy logic is used to convert data values into ranges, and each of these ranges is then processed via a rule engine for reducing processing complexity.

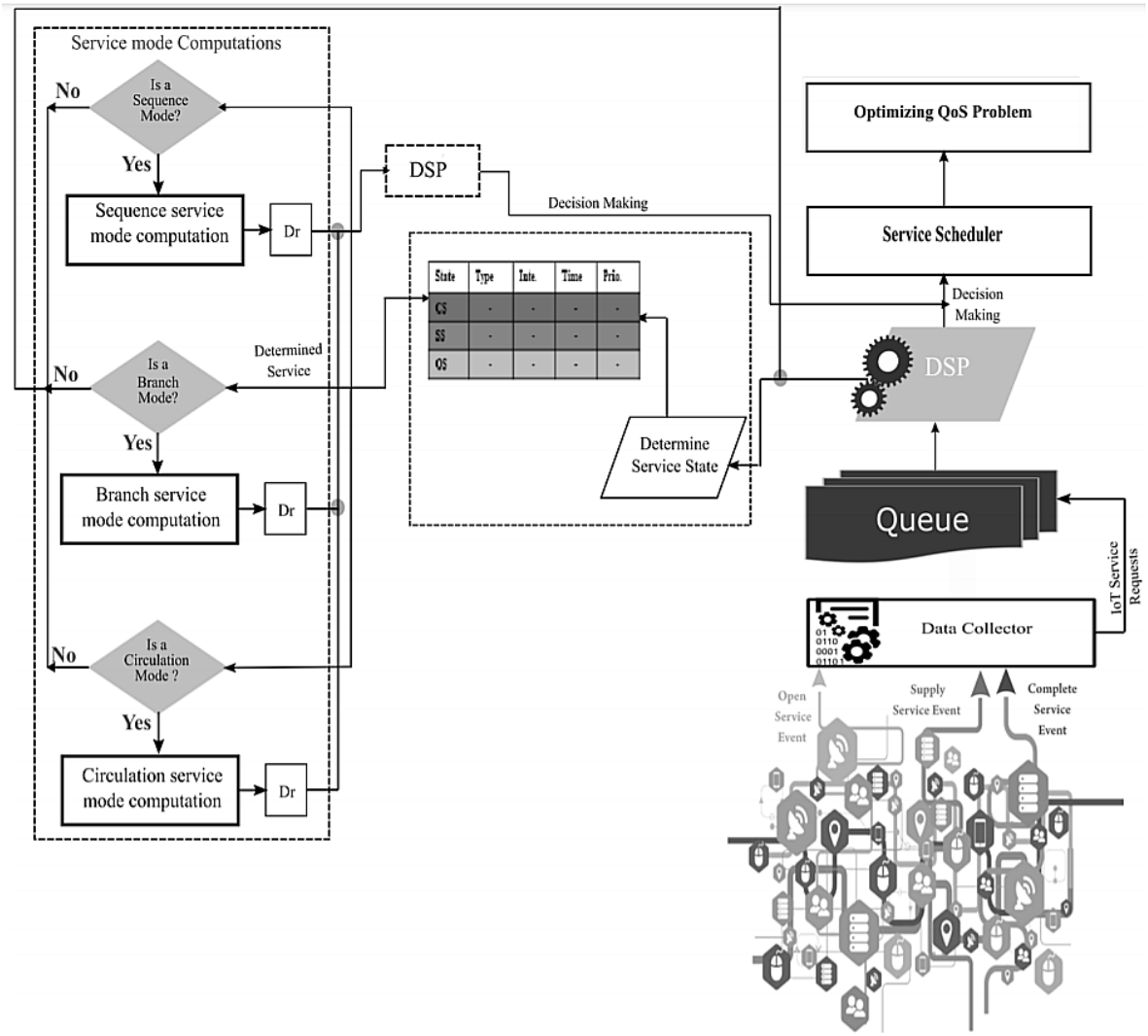


Figure 3.2. Architecture to improve quality of service (QoS) for healthcare IoT devices [15]

3.3 Improve quality of service (QoS) for healthcare IoT devices

Personalized health care systems are designed for patients with severe chronic conditions, wherein each system is specifically designed for solving a patient specific issue. For instance, patients with chronic kidney diseases are provided with intrusive indigestible sensors, which can sit beside the kidney to continuously monitor its real-time performance. Based on this performance real time continuous kidney function test (RTCKFT) is performed. This test allows medical practitioners to continuously monitor body parameters, and to reduce dependency on inaccurate test labs. A brief study of these sensors which includes development of Micro-Electro-Mechanical Systems (MEMS), Decision tree with NSUM models, cognitive skill evaluation, adaboost for carcinogenic conditions, fuzzy logic for Alzheimer detection, diabetic retinopathy detection, adaptive reproductive management, and chest disease monitoring can be observed from [18, 19].

All these models suggest specific systems for continuously monitoring body parameters to improve overall system efficiency.

Parallel computations can also be used for improved Internet of Things Quality-of-Service performance. [20] provides an example of a system that uses parallel processing architectures to increase quality of service. Internet of Things-based healthcare solutions, such as implanted and wearable body sensor networks, use parallel processing. Using data on children's health and digital toys, a model of distributed behavior orchestration in the Internet of Things' cognitive solution is presented. In a distributed health information system, big data, complicated event processing, provenance of the Internet of Things, and traceability of wearable data streams By utilising fog-based middleware, the Internet of Health Things can abide by the privacy guidelines set forth by the Organisation for Economic Cooperation and Development. Cooperative end-to-end key management for e-health, Internet of Things-based, evidence-based, and community health service architecture-based non-contact health monitoring. All these models showcase an improvement of 20% in terms of computational efficiency when compared to a non-parallel architecture. The work in [21] gives light to other healthcare applications which use internet of things-based systems, and discusses the types of attacks, performance issues, etc. which can be worked upon via application of IoT to the system.

Work in [22] discusses a multi-hop architecture that uses cooperative computing for load balancing of IoT data over cloud. This load balancing includes offloading the entire computational load on the cloud, via which the overall computational efficiency can be improved. Moreover, due to the multi-hop cooperative-messaging mechanism Nash equilibrium is obtained with quality-of-service awareness. Each Internet of Things device is connected to the cloud (base station) via other Internet of Thing devices, via peer-to-peer communication. These devices use a broadcasting mechanism to evaluate nearby nodes, and then communicate their data over to the base stations via these nearby nodes. The usage of this multi-hop communication interface results in performance improvements of 15% in terms of communication delay and 5% in terms of overall energy consumption. This approach also assists in service discoverability as discussed in [23], wherein Genetic Algorithm (GA) is used to evaluate best service routing paths for any given internet of things application. The technique, known as Genetic technique based QoS global optimisation and dynamic replanning web service selection algorithm (GODRP), can represent an endless number of service combinations for better system performance in terms of quality-of-service. This quality-of-service includes delay needed

for computation, accuracy of disease detection, throughput of communication and other quality parameters. A similar algorithm is developed in [24] and uses mixed-integer linear programming (MILP) which avoids repetitive computations, thereby improving overall quality-of-service for the system. Other works in [25], [26], [27], [28] and [29] highlight on different clinical issues with healthcare internet-of-things devices, enabling blockchain into internet-of-things devices to resolve security issues in the network, embedding deep learning into internet-of-things devices for improved human activity recognition performance, evaluation of attacks like forgery attacks & remote authentication attacks on internet-of-things devices and then securing these devices from these attacks via cloud centric internet-of-medical-things devices for smart healthcare. But these articles do not provide the design for a comprehensive system for improving health monitoring by taking into consideration environmental effects on human health conditions.

Researchers have provided a wide range of blockchain models, and each model has distinct characteristics in terms of the performance and operational metrics it uses. For example, the research discussed in [5, 6] suggests using a variety of different blockchain consensus models in addition to Software Defined Network (SDN) for low delay, reliable, and secure models with powerful emergency handling capabilities (LSRDM-EH), which can be used for real-time deployments. These models cannot be scaled up for use in large-scale deployments since they employ methods of high complexity for developing healthcare applications. According to a study published in [7], automation in procurement contracts (APC) is suggested as a solution for this restriction and to increase its utilisation. The solution automates the processes for upgrading them by utilising smart contracts and low-complexity decision-making techniques. Researchers in [8, 9], [10], and [11] investigate the use of Consortium Blockchains, Edge Computing with Blockchains (ECB), and Attribute-Based Searchable Encryption for Blockchain-based Search Applications (ABSE2). These models help to improve storage capacity for a variety of healthcare applications by leveraging data augmentation and redundancy control. Some expansions to these principles that are being researched include Blockchain Logging Contracts (BLCs), Permissioned Blockchains with Security Risk Management (SRM), Lattices-based Cryptography with Deep Learning (LCDL), and Machine Learning (ML) blockchains. To boost QoS performance in response to different assault kinds, these models use high density feature extraction and classification techniques.

Researchers are also looking on techniques to strengthen defences against various kinds of network attacks. These techniques are taken into consideration alongside techniques

that help raise security levels while maintaining context-aware performance. As part of the examination of these models, [15, 16], [17], and [18] discuss the usage of Software-Defined Infrastructure for blockchains, Patient-Centric Blockchains, and Confidential Group Transactions, which allow for improved performance under a range of specific use scenarios. Researchers have created similar models employing Elliptic Curve Cryptography (ECC), the Edwards-Curve Digital Signature Algorithm (EdDSA) for hybrid cryptography, autonomous encryption-decryption (AED) [18], blockchain-based edge computing (BEC), and hybrid cryptography [19]. These models employ extremely advanced encryption and processing methods, limiting their potential to scale when employed across a large number of institutions. Ring Signature and Stealth Address (RSSA), Decoupled Processing, and multilayer models should be used in the works of [21], [22], and [23] to include scalability-aware techniques that can be optimised based on the number of block requests. Here are some suggestions for enhancing its performance. Scalable blockchains [24] and reinforced blockchains (FBs) [25] allow to further develop these models by combining privacy protection and precise access control for a number of applications. Accordingly, [24] and [25]. However, these models employ difficult encryption methods, which limit the amount of service quality that IoMT devices can provide.

3.4 Summary

This section highlighted other health concerns that conventional healthcare models must address as our society ages, such as the increased incidence of chronic diseases, the rising cost of clinical and hospital treatments, and other related difficulties. Effective and efficient medical systems must be built in order to lower healthcare costs, increase treatment quality, and ease pressure on hospital systems and healthcare professionals. The potential for IoT-based remote healthcare monitoring technologies is huge. This paper evaluated earlier Internet of Things investigations and proposed an IoTTA architecture. The models shown are a representation of the technology and frameworks in use today. But in the research that were analyzed, various IoTTA tiers were applied in various ways. According to the review's results, the next wave of IoT applications for healthcare should focus primarily on machine learning, data mining, and self-care. Future research will focus on developing a falls detection and prevention system using the IoTTA technique, as well as data collection and analysis. Given that they outperformed other models in terms of performance levels, deep learning and bioinspired models were heavily utilised in this work to solve a range of IoT-related issues in clinical use cases.

CHAPTER 4

Improving Efficiency of IoT-Based Healthcare Monitoring

4.1 Utilising deep learning models to increase the efficiency of IoT-based healthcare monitoring and control devices.

Improving efficiency of IoT-based healthcare monitoring and control devices using deep learning models.

The Internet of Things (IoT) is a boon to the healthcare business due to its inherent benefits such as remote monitoring, remote actuation, high-speed data processing, and inexpensive operating costs. Doctors globally employ IoT devices such as electrocardiogram (ECG) monitors, continuous blood pressure (CBP) monitors, continuous oxygen level monitors, and so on to properly monitor patient status and decrease overheads on the currently overworked nursing staff. Due to the great availability of processing resources and restricted power constraints at hospitals and other healthcare facilities, IoT devices can improve their performance through high precision temporal data analysis and decision making in the event of even minor irregularities. Some of the newest IoT systems have integrated such high accuracy algorithms to enhance their usefulness in real-time monitoring and control. However, older systems must be changed to improve their performance, which poses a number of challenges, including but not limited to the cost of replacement, calibration, familiarity of nursing staff with old equipment, etc. To reduce the effect of these challenges, this chapter provides a revolutionary high accuracy, highly interfaceable, and low-cost deep learning solution that can be combined with both old and new healthcare monitoring devices to increase efficiency. Certain minimal application criteria are set for a device to be qualified for interfacing, and it has been noted that this design can update more than 80% of existing operational healthcare devices, improving monitoring and control effectiveness. The system architecture has been shown to be more than 99% accurate in terms of parameter monitoring, as well as outstanding control exercising capabilities.

4.2 Introduction to the model

The created devices need to follow specific guidelines in order to execute IoT-based health care monitoring with high speed, high accuracy, and high performance. High precision monitoring, insightful analysis, and effective control are some of these guiding ideas. For completing these tasks, numerous algorithms have been developed, and each

approach has unique nuances, benefits, and drawbacks. To properly comprehend the process of data flow in healthcare IoT, IoT components such as sensors, storage devices, analytical processing algorithms, cloud installations, and actuation points must be thoroughly examined. Figure 4.1 displays the data flow in a typical healthcare IoT system, which includes sensors, storage units, analytical processing units, cloud interfaces, and actuating entities (Doctors), from devices to storage to reporting. Any IoT healthcare system functions in the ways that are outlined here.

Information gathering and storage from wearable and non-wearable gadgets, such as blood pressure monitors, oxygen monitors, temperature monitors, and ECG sensors, etc. Next, this data will be processed in greater detail using the cloud. Every IoT device for healthcare data collecting has two basic purposes.

- To minimise any reading errors caused during data collecting, pre-processing programmes like averages and adaptive median filters.
- To use data storage standards like Java Simple Object Notation (JSON) and XML to ensure quick access, clarity, and security. Encryption, hashing, data framing, secret sharing, and other techniques are used to protect information from internal and external dangers.

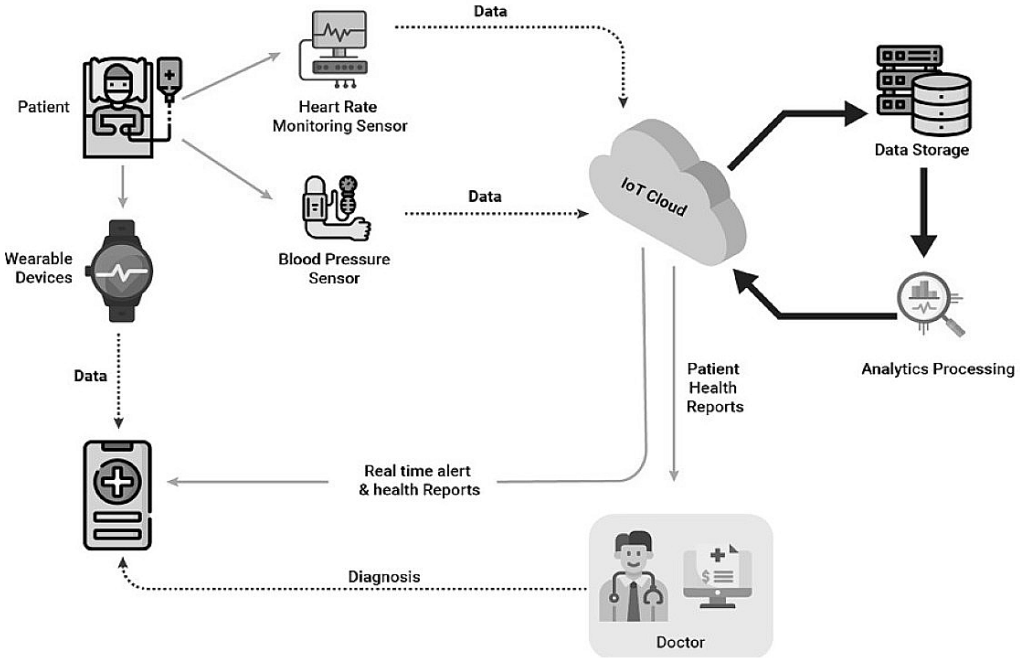


Figure 4.1. A typical healthcare IoT data flow

- The IoT cloud layer collects and stores data from capturing devices. The storage device needs ordered files or rows and columns for this data. Some IoT cloud

installations, like from Azure and Google Cloud, allow unstructured content and eventually convert it into their own unique internal format, which enables them to quickly access this information via indexing when appropriate. This is accomplished using databases such as MySQL (Structured Query Language), Firebase, etc.

- An analytical processing unit receives data from various databases and applies OLAP [1] techniques, such as aggregation, partitioning, and data cube processing, to it. One of the most important elements in the system, its effectiveness defines the action plans that doctors will use to improve the health of their patients. Deep learning techniques are utilised for this, including Q-Learning, Support Vector Machines (SVM), and Convolutional Neural Networks (CNNs).
- The cloud is sent with the processed data, which uses it to update the medical facility's and the doctor's equipment with information about patient conditions. In order to create reports and create action plans, this conclusion is employed. Algorithms [2] as labelling, categorising, grouping, etc. are used to provide high-quality reports. These algorithms give the system useful methods to display data, enhancing user experience and data visualisation effectiveness.
- Additional processing is carried out to improve the patient's health based on these findings. The system's effectiveness is assessed following each report when this process is repeated. Corrective measures are done based on this effectiveness so that the patient's health can be proven to improve.

A healthcare IoT system is to be functional, each of these building blocks must be developed as efficiently as possible. This chapter covers the architecture for constructing these blocks with amazing efficiency as well as improving the functionality of existing healthcare IoT blocks. The characteristics, benefits, and downsides of present healthcare IoT systems must be assessed before developing the proposed solution. This assignment is completed in the next section by examining many current IoT deployment tactics and assessing their performance in terms of decision-making accuracy, reaction time, application domain, and so on. The next step is to design and analyse the proposed architecture. The concluding section of this chapter offers some notable observations about the suggested architecture. The final section of this chapter includes some noteworthy observations regarding the suggested architecture and suggestions for making it better.

4.3 Design of the proposed model

The suggested model uses both external and internal parameters for monitoring and control in order to increase the effectiveness of internet-of-things-based healthcare monitoring and control. Figure 4.2 shows this paradigm, which includes several components for monitoring, controlling, and optimising.

The architecture works using via the following steps,

- Environmental parameters like temperature, humidity, gas levels and pressure levels are extracted via environmental sensors. The following are the applications for extraction of these parameters.

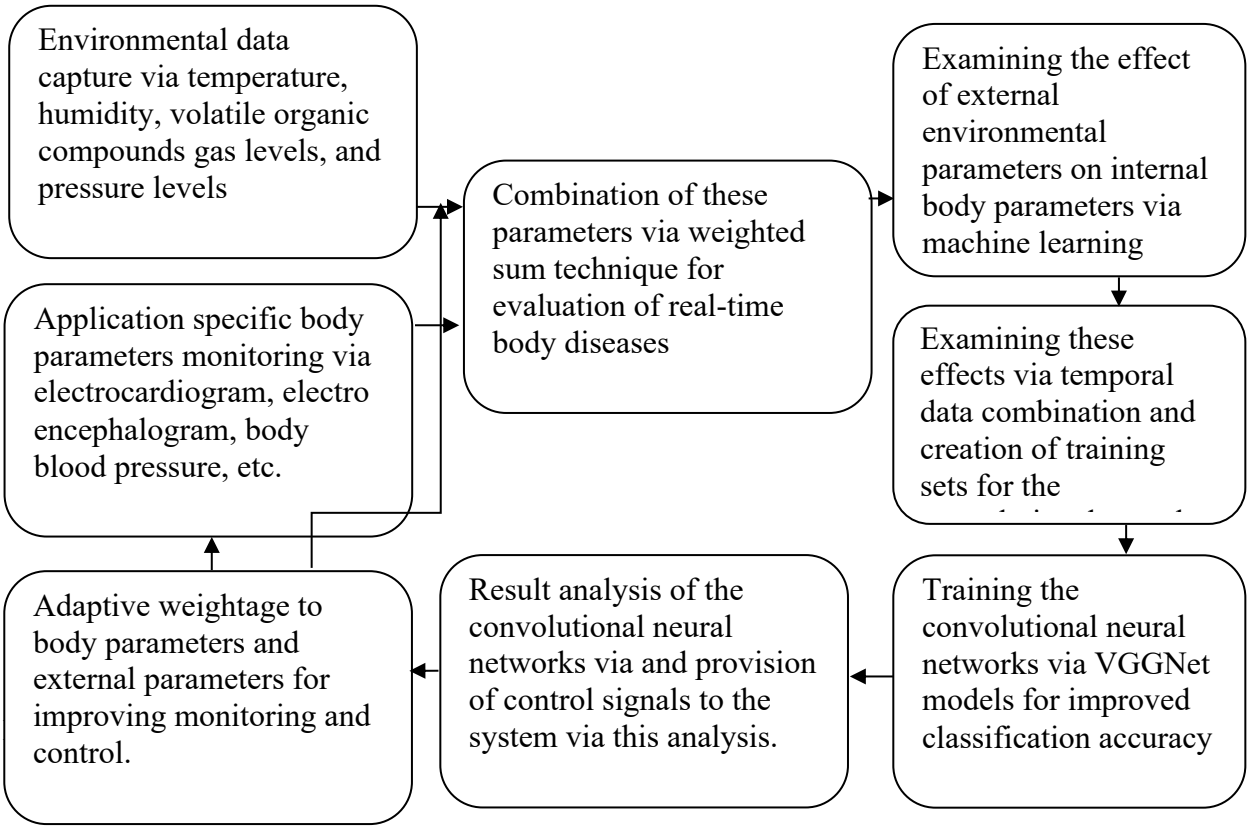


Figure 4.2. Architecture of the proposed healthcare IoT monitoring and control system.

The architecture works using via the following steps,

- Environmental parameters like temperature, humidity, gas levels and pressure levels are extracted via environmental sensors. The following are the applications for extraction of these parameters,
    - Mortality rates are higher in high & low temperatures, than it is at moderate temperatures. Thus, effect of temperature on health condition must be considered.
    - Humidity controls overall liquid flow in human body. A highly humid atmosphere causes a large amount of water to come out of the body.
    - Gas levels cause interim effects in long term for patients with existing conditions, thus these parameters must also be considered while performing health analysis.
    - Pressure levels cause headaches, shortness of breath, and other health effects. These effects can cause nausea, anxiety, and other issues to the patients.
- Application specific body sensors are deployed, depending upon the patient's condition. The following sensors are used for each use case,
    - ECG sensors are used for heart monitoring.
    - EEG sensors are used for brain activity monitoring.
    - EMG sensors are used for muscle movement monitoring.
    - Blood pressure sensors are used for monitoring changes in heartbeat.
    - Body gas sensors are used to evaluate gas levels in the body.
    - Imaging sensors are used for the following external visual clues,
        - Facial imaging sensors are used to indicate any changes in facial skin tone, fatigue, etc.
        - Skin disease detection sensors are used to evaluate moles and other skin conditions.
        - Continuous drowsiness monitoring is done via the use of specialized facial features.
    - Implant sensors are used for continuous monitoring of different parameters like kidney function, blood pressure, etc.
    - Glucose monitoring devices are used to monitor sugar levels in the body.

- A combination of these sensors is done, and weighted sum technique is used for evaluating total feature vector for the body. This feature vector consists of both the body parameters and the environmental parameters. Application specific selection can be done for both body and environmental parameters.
- An evaluation engine is deployed which is based on convolutional neural networks for evaluating the kind of disease or body condition the patient is suffering from, and this is showcased to the patient via high-speed communication interface.
- The body condition data is linked with environmental data and is stored in the database for temporal analysis. Each of these storage units consists of the following combination of data,
    - ECG dependence on environmental temperature
    - ECG dependence on environmental humidity
    - ECG dependence on environmental pressure
    - ECG dependence on environmental gas levels
    - EEG dependence on environmental temperature
    - EEG dependence on environmental humidity
    - EEG dependence on environmental pressure
    - EEG dependence on environmental gas levels
    - EMG dependence on environmental temperature
    - EMG dependence on environmental humidity
    - EMG dependence on environmental pressure
    - EMG dependence on environmental gas levels
    - Blood pressure dependence on environmental temperature
    - Blood pressure dependence on environmental humidity
    - Blood pressure dependence on environmental pressure
    - Blood pressure dependence on environmental gas levels
    - Body gas levels dependence on environmental temperature
    - Body gas levels dependence on environmental humidity
    - Body gas levels dependence on environmental pressure
    - Body gas levels dependence on environmental gas levels
    - Saturated Oxygen level dependence on environmental temperature
    - Saturated Oxygen level dependence on environmental humidity

  - Saturated Oxygen level dependence on environmental pressure
  - Saturated Oxygen level dependence on environmental gas levels
  - Glucose level dependence on environmental temperature
  - Glucose level dependence on environmental humidity
  - Glucose level dependence on environmental pressure
  - Glucose level dependence on environmental gas levels
  - Kidney function dependence on environmental temperature
  - Kidney function dependence on environmental humidity
  - Kidney function dependence on environmental pressure
  - Kidney function dependence on environmental gas levels
  - Liver function dependence on environmental temperature
  - Liver function dependence on environmental humidity
  - Liver function dependence on environmental pressure
  - Liver function dependence on environmental gas levels
  - Facial parametric dependence on environmental temperature
  - Facial parametric dependence on environmental humidity
  - Facial parametric dependence on environmental pressure
  - Facial parametric dependence on environmental gas levels
  - Skin disease level dependence on environmental temperature
  - Skin disease level dependence on environmental humidity
  - Skin disease level dependence on environmental pressure
  - Skin disease level dependence on environmental gas levels
  - Lung function dependence on environmental temperature
  - Lung function dependence on environmental humidity
  - Lung function dependence on environmental pressure
  - Lung function dependence on environmental gas levels
- All these dependency levels are given to a VGGNet based neural network for training. Which results into a system where output determines the level of effect of every-body parameter on the resulting external parameter.
- Using the training results, control signals are generated which assist in identifying the level of impact of these parameters and suggest their effects to the patient in table 4.1.

- Based on these signals patients are alerted to either stay indoors or move outdoors depending upon their health conditions.
- The following table indicates patient's health conditions, environmental conditions, and the resulting inference of these conditions for control signal passing.
- These rules are updated as number of samples are increased and the training set, and temporal data is added to the system.
- Depending upon these rules, patients are advised either to shift to a better area or stay at their current environmental location.

Table 4.1: Example of rules given to the patient based on their current condition.

Current patient condition	**Current environmental condition**	**Inference signal given to the patient**
Sweaty	Humid	Move indoors in a cool place
High temperature	Hot	Move indoors in a cool place
Normal temperature	Hot	Stay in the current environment
Non sweaty	Humid	Stay in the current environment
Itching in the body	Hot	Move to a cooler place
Itching in the body	Humid	Move to a cool place with low humidity

- Parameters are re-evaluated and the process goes on continuing, until there is an improvement in the patient's body parameters.
- Such a kind of environmental linkage assists in improving overall patient health.
- The following machine learning model is used to choose the ideal setting for the patient,
    - Input
        - Number of iterations (Ni)
        - Number of solutions (Ns)
        - Learning factor (Lf)
        - Maximum number of locations available for the patient to be shifted (Lmax).
    - Algorithm,
        - Initially mark all solutions as 'to be changed'.

- For each iteration,
  - For each solution which is marked as ‘to be changed’,

- Shift the patient to a random location from 1 to Lmax
- Evaluate environment parameters, and patient’s body parameters in this location.
- Find the fitness value for this patient using the following formula,

$$F_i = f_1(Int.) * f_2(Ext.) \quad (4.1)$$

Where, Int. and Ext. are internal and external parameters, and f_1 & f_2 are internal and external parametric evaluation functions. These activities can be seen in the case study portion of this chapter and vary depending on the health condition being tracked.

- Next, determine the average fitness value before determining the fitness threshold value,

$$F_{th} = \frac{\sum_{i=1}^{N_S} F_i}{N_S} * Lr \quad (4.2)$$

- Discard all solutions which have lower than threshold fitness, and pass other solutions to next iteration,
  - Use the solution with maximum fitness and shift the patient to that particular location.
- Continuously monitor patient data, and if fitness goes below a certain threshold, then shift patient to the next best fitness solution. Repeat this process for all patients.

- The following case-study can be used for patients who are suffering from CoVID,
  - Input
    - Number of iterations (Ni)
    - Number of solutions (Ns)
    - Learning factor (Lf)
    - Maximum number of hospital beds available for the patient to be shifted (Lmax).
  - Algorithm,
    - Initially mark all solutions as ‘to be changed’.
    - For each iteration,
      - For each solution which is marked as ‘to be changed’,

- Shift the patient to a random bed from 1 to Lmax
- Evaluate environment parameters, and patient's body parameters in this location.
- Find the fitness value for this patient using the following formula,

$$F_i = \frac{(T_2 - T_1)}{T_2} * \frac{O_2 - O_1}{O_2} * \frac{(T_{ext2} - T_{ext1})}{T_{ext2}} \quad (4.3)$$

Where, 'T' and 'O' are the values of temperature and oxygen levels for the patient at different time instants, and T_{ext} is the external temperature for the same time instant.

- Next, determine the average fitness value before determining the fitness threshold value,

$$F_{th} = \frac{\sum_{i=1}^{N_S} F_i}{N_S} * Lr \quad (4.4)$$

- Discard all solutions which have lower than threshold fitness, and pass other solutions to next iteration,
  - Use the solution with maximum fitness and shift the patient to that particular hospital bed.
  - Continuously monitor patient data, and if fitness goes below a certain threshold, then shift patient to the next best fitness solution. Repeat this process for all patients.
- The following case-study can be used for patients who are suffering from Heart Disease,
  - Input
    - Number of iterations (Ni)
    - Number of solutions (Ns)
    - Learning factor (Lf)
    - Maximum number of hospital beds available for the patient to be shifted (Lmax).
  - Algorithm,
    - Initially mark all solutions as 'to be changed'.
    - For each iteration,
      - For each solution which is marked as 'to be changed',

- Shift the patient to a random bed from 1 to Lmax
- Evaluate environment parameters, and patient's body parameters in this location.
- Find the fitness value for this patient using the following formula,

$$F_i = \frac{(ECG_2 - ECG_1)}{ECG_2} * \frac{BP_2 - BP_1}{BP_2} * \frac{(T_{ext2} - T_{ext1})}{T_{ext2}} * \frac{(H_{ext2} - H_{ext1})}{H_{ext2}} \quad (4.5)$$

Where, 'ECG' and 'BP' are the values of ECG and blood pressure levels for the patient at different time instants, and T_{ext} is the external temperature for the same time instant, while H is the external humidity for the same time instant.

- Next, determine the average fitness value before determining the fitness threshold value,

$$F_{th} = \frac{\sum_{i=1}^{N_S} F_i}{N_S} * Lr \quad (4.6)$$

- Discard all solutions which have lower than threshold fitness, and pass other solutions to next iteration,

- Use the solution with maximum fitness and shift the patient to that particular hospital bed.
- Continuously monitor patient data, and if fitness goes below a certain threshold, then shift patient to the next best fitness solution. Repeat this process for all patients.

- The following case-study can be used for patients who are suffering from Diabetes,
  - Input
    - Number of iterations (Ni)
    - Number of solutions (Ns)
    - Learning factor (Lf)
    - Maximum number of locations available for the patient to be shifted (Lmax).
  - Algorithm,
    - Initially mark all solutions as 'to be changed'.
    - For each iteration,
      - For each solution which is marked as 'to be changed',
  - Shift the patient to a random bed from 1 to Lmax
  - Evaluate environment parameters, and patient's body parameters in this location.
  - Find the fitness value for this patient using the following formula,

$$F_i = \frac{(GL_2 - GL_1)}{GL_2} * \frac{O_2 - O_1}{O_2} * \frac{(T_{ext2} - T_{ext1})}{T_{ext2}} * \frac{(H_{ext2} - H_{ext1})}{H_{ext2}} \quad (4.7)$$

Where, 'GL' and 'O' are the values of glucose and oxygen levels for the patient at different time instants, and T_{ext} is the external temperature for the same time instant,

while H is the external humidity for the same time instant.

- Next, determine the average fitness value before determining the fitness threshold value,

$$F_{th} = \frac{\sum_{i=1}^{N_S} F_i}{N_S} * Lr \quad (4.8)$$

- Discard all solutions which have lower than threshold fitness, and pass other solutions to next iteration,
- Use the solution with maximum fitness and shift the patient to that particular hospital bed.
- Continuously monitor patient data, and if fitness goes below a certain threshold, then shift patient to the next best fitness solution. Repeat this process for all patients.

- As it can be observed, major chunk of algorithm remains the same, but changes are made in fitness function levels. These fitness function levels decide the rate of change of the environmental and human body parameter, and how to minimize it for best results.
- Lower change in these values, will result in stabler patient condition, and thereby improve the patients' health quickly.

In order to evaluate the performance of this system, the system was tested on different categories of patients with different health conditions. These results are tabulated in the next section.

4.4 Result Analysis and Comparisons

Different testing conditions were used to evaluate the results for the specified algorithm. Patients with these disorders include those who have four separate types of mutually exclusive diseases, including,

- High blood sugar
- Cardiovascular issues
- Lung Cancer
- Diabetic retinopathy

A large number of patients were used for this evaluation, and results for number of days needed for improvement of patient's health were recorded. Expected values for these patients are evaluated (using Python based simulation), and results were tabulated, actual results are used for initial 50 patients and 6-month duration, and then the results are interpolated for obtaining an approximate value of the same. Similar observations were

inferred from the work in [11] and [15], and the following results shown in table 4.2 and figure 4.3 were seen,

Table 4.2 Recovery duration for patients with high blood sugar levels

Number of patients with High Blood sugar	**Expected Average by using recovery [11]**	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model**
5 Patients	5 days	4.5 days	3 days
10 Patients	4.5 days	4.3 days	3.1 days
15 Patients	4.9 days	4.7 days	2.9 days
20 Patients	5.5 days	4.9 days	3.8 days
25 Patients	5.9 days	6.2 days	3.7 days
30 Patients	3.8 days	3.7 days	2.1 days
35 Patients	5.2 days	5.5 days	2.5 days
40 Patients	5.1 days	4.9 days	2.8 days
45 Patients	6.8 days	7.5 days	3.7 days
50 Patients	6.5 days	5.4 days	3.4 days
60 Patients	8 days	7.5 days	4.5 days
70 Patients	5.8 days	5.4 days	3.8 days
80 Patients	6.5 days	7.2 days	4.9 days
90 Patients	8.5 days	8.8 days	3.5 days
100 Patients	6.5 days	7.6 days	2.8 days
110 Patients	9.5 days	8 days	3.5 days
120 Patients	12 days	8 days	5.6 days
130 Patients	13 days	9 days	5.8 days
140 Patients	12 days	14 days	8.9 days
150 Patients	5.4 days	5.9 days	3.8 days
160 Patients	10 days	8 days	4.3 days
170 Patients	15 days	9 days	6.8 days
180 Patients	9 days	6.5 days	4 days
190 Patients	16 days	15 days	9 days
200 Patients	3.8 days	2.9 days	1.3 days

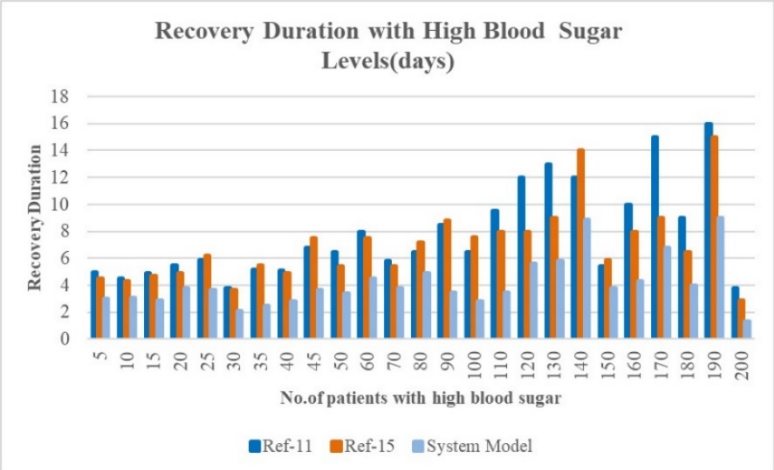


Fig 4.3 Recovery duration for patients with high blood sugar levels

Similar comparison was made for patients with cardio-vascular disease, and the following results were obtained as shown in table 4.3 and figure 4.4,

Table 4.3. Recovery duration for patients with cardio-vascular disease

Number of patients with Cardiovascular disease	**Expected Average recovery by using [11]**	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model**
5 Patients	4 months	3.5 months	2 months
10 Patients	4.5 months	4.3 months	3.1 months
15 Patients	4.9 months	4.7 months	2.9 months
20 Patients	5.5 months	4.9 months	3.8 months
25 Patients	5.9 months	6.2 months	3.7 months
30 Patients	3.8 months	3.7 months	2.1 months
35 Patients	5.2 months	5.5 months	2.5 months
40 Patients	5.1 months	4.9 months	2.8 months
45 Patients	6.8 months	7.5 months	3.7 months
50 Patients	6.5 months	5.4 months	3.4 months
60 Patients	8 months	7.5 months	4.5 months
70 Patients	5.8 months	5.4 months	3.8 months
80 Patients	6.5 months	7.2 months	4.9 months
90 Patients	8.5 months	8.8 months	3.5 months
100 Patients	6.5 months	7.6 months	2.8 months
110 Patients	9.5 months	8 months	3.5 months
120 Patients	12 months	8 months	5.6 months

130 Patients	13 months	9 months	5.8 months
140 Patients	12 months	14 months	8.9 months
150 Patients	5.4 months	5.9 months	3.8 months
160 Patients	10 months	8 months	4.3 months
170 Patients	15 months	9 months	6.8 months
180 Patients	9 months	6.5 months	4 months
190 Patients	16 months	15 months	9 months
200 Patients	3.8 months	2.9 months	1.3 months

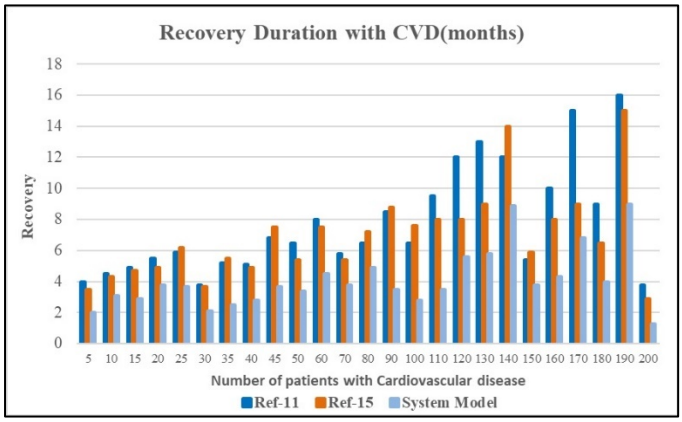


Figure 4.4. Recovery duration for patients with cardio-vascular disease

Another comparison was made for patients with lung cancer, and the following results were obtained as shown in table 4.4 and figure 4.5.

Table 4.4 Recovery duration for patients with lung cancer condition

Number of patients with Lung cancer condition	**Expected Average recovery by using [11]**	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model**
5 Patients	5 fortnights	4.5 fortnights	3 fortnights
10 Patients	4.5 fortnights	4.3 fortnights	3.1 fortnights
15 Patients	4.9 fortnights	4.7 fortnights	2.9 fortnights
20 Patients	5.5 fortnights	4.9 fortnights	3.8 fortnights
25 Patients	5.9 fortnights	6.2 fortnights	3.7 fortnights
30 Patients	3.8 fortnights	3.7 fortnights	2.1 fortnights
35 Patients	5.2 fortnights	5.5 fortnights	2.5 fortnights
40 Patients	5.1 fortnights	4.9 fortnights	2.8 fortnights
45 Patients	6.8 fortnights	7.5 fortnights	3.7 fortnights

50 Patients	6.5 fortnights	5.4 fortnights	3.4 fortnights
60 Patients	8 fortnights	7.5 fortnights	4.5 fortnights
70 Patients	5.8 fortnights	5.4 fortnights	3.8 fortnights
80 Patients	6.5 fortnights	7.2 fortnights	4.9 fortnights
90 Patients	8.5 fortnights	8.8 fortnights	3.5 fortnights
100 Patients	6.5 fortnights	7.6 fortnights	2.8 fortnights
110 Patients	9.5 fortnights	8 fortnights	3.5 fortnights
120 Patients	12 fortnights	8 fortnights	5.6 fortnights
130 Patients	13 fortnights	9 fortnights	5.8 fortnights
140 Patients	12 fortnights	14 fortnights	8.9 fortnights
150 Patients	5.4 fortnights	5.9 fortnights	3.8 fortnights
160 Patients	10 fortnights	8 fortnights	4.3 fortnights
170 Patients	15 fortnights	9 fortnights	6.8 fortnights
180 Patients	9 fortnights	6.5 fortnights	4 fortnights
190 Patients	16 fortnights	15 fortnights	9 fortnights
200 Patients	3.8 fortnights	2.9 fortnights	1.3 fortnights

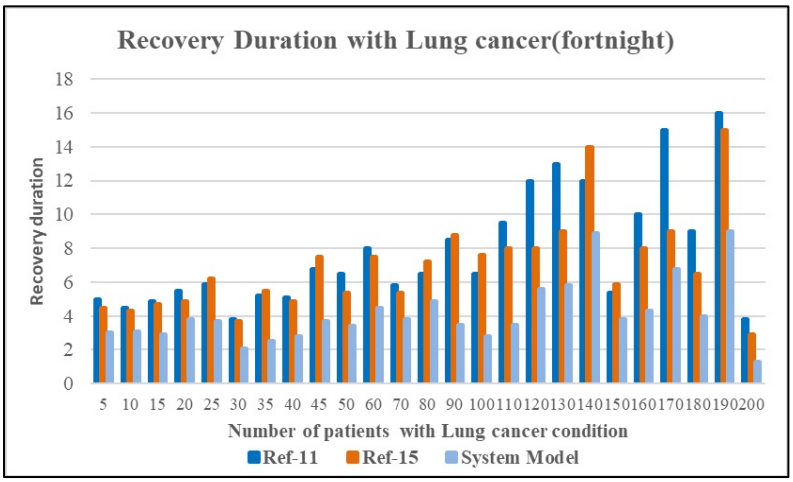


Figure 4.5 Recovery duration for patients with lung cancer condition

Another comparison was made for patients with diabetic retinopathy, and the following results were obtained as shown in table 4.5 and figure 4.6,

Table 4.5. Recovery duration for patients with diabetic retinopathy condition

Number of patients with Diabetic Retinopathy condition	**Expected Average recovery by using [11]**	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model**
5 Patients	5 weeks	4.5 weeks	3 weeks
10 Patients	4.5 weeks	4.3 weeks	3.1 weeks
15 Patients	4.9 weeks	4.7 weeks	2.9 weeks
20 Patients	5.5 weeks	4.9 weeks	3.8 weeks

25 Patients	5.9 weeks	6.2 weeks	3.7 weeks
30 Patients	3.8 weeks	3.7 weeks	2.1 weeks
35 Patients	5.2 weeks	5.5 weeks	2.5 weeks
40 Patients	5.1 weeks	4.9 weeks	2.8 weeks
45 Patients	6.8 weeks	7.5 weeks	3.7 weeks
50 Patients	6.5 weeks	5.4 weeks	3.4 weeks
60 Patients	8 weeks	7.5 weeks	4.5 weeks
70 Patients	5.8 weeks	5.4 weeks	3.8 weeks
80 Patients	6.5 weeks	7.2 weeks	4.9 weeks
90 Patients	8.5 weeks	8.8 weeks	3.5 weeks
100 Patients	6.5 weeks	7.6 weeks	2.8 weeks
110 Patients	9.5 weeks	8 weeks	3.5 weeks
120 Patients	12 weeks	8 weeks	5.6 weeks
130 Patients	13 weeks	9 weeks	5.8 weeks
140 Patients	12 weeks	14 weeks	8.9 weeks
150 Patients	5.4 weeks	5.9 weeks	3.8 weeks
160 Patients	10 weeks	8 weeks	4.3 weeks
170 Patients	15 weeks	9 weeks	6.8 weeks
180 Patients	9 weeks	6.5 weeks	4 weeks
190 Patients	16 weeks	15 weeks	9 weeks
200 Patients	3.8 weeks	2.9 weeks	1.3 weeks

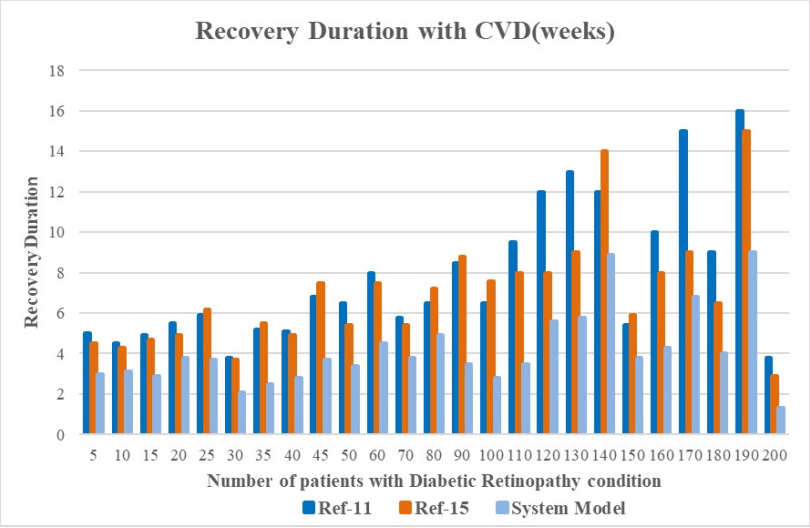


Figure 4.6. Recovery duration for patients with diabetic retinopathy condition

Thus, from the results it may be determined that the model performs better in terms of recovery rates than other models. This is primarily because the suggested model uses both internal and external parameters to assess patient circumstances, which tends to enhance such conditions through high speed and high accuracy. model for machine learning.

4.5 Conclusion

Individual models for CoVID, heart disease and diabetes are mentioned in this text, which allow system designers to evaluate and design their healthcare IoT systems for improved overall system performance. These models are tested on a variety of datasets and for a wide spectrum of patients. In all cases, the system outperformed existing systems, and showcased a 15% faster improvement in overall patient's health. The system is tested against 4 different types of diseases, and it is evaluated that for every disease speed of patient's condition improvement is better when using the system model. But the model can be further improved via testing it on larger number of patients, and also by doing better deep dive into system performance by considering a larger number of diseases. Moreover, use of complex deep learning models can also be done for better evaluation of the system when number of diseases are increased.

CHAPTER 5

Quality of service (QoS) Awareness For Safe Healthcare Deployments using IoT Network .

5.1 Design of a unique sidechain-based IoT network for QoS secure healthcare system.

Networks called the Internet of Medical Things (IoMT) are focused on designing secure, low-latency healthcare communication interfaces. To provide such interfaces, effective models for privacy, hashing, data encryption, and quality of service (QoS) awareness are needed. Various standard medical interfaces have been created by researchers to reduce network redundancy and enable high-throughput and a low latency communications. Additionally, security models are used by these interfaces to ensure data encryption and privacy. Nevertheless, the QoS performance of the IoMT devices is decreased by the use of encryption techniques, which restricts the use of these devices for in-patient monitoring and treatment in real-time. In order to improve IoMT QoS while maintaining high security, this book presents the design of QSIH, a QoS-aware sidechain architecture that may be used for protecting IoMT networks. The suggested approach explains how to create a data storage and communication interface based on blockchain technology that can eliminate a range of network assaults. With each new block added to the system, the communication time required in any blockchain-based interface grows dramatically. A new genetic algorithm-based machine learning model optimisation is suggested to lessen this delay. The suggested methodology ensures low latency and high communication throughput by splitting the primary blockchain into many shards in a QoS-aware way. Using interactive Q-Learning (IQL), which can enlarge or contract these chains based on the QoS performance of the network, the shards (or sidechains) are maintained. The network's preservation requirements determine how the network merges the archived sidechains with other sidechains after they are created from the main blockchain. The system QSIH paradigm might increase throughput by 14%, decrease storage costs by 5%, and cut network communication time by 18%, and because of the dynamic sidechaining architecture, the network can retain a high level of security and privacy. After putting the model through a number of IoMT scenarios, different network simulations revealed that it performed consistently.

5.2 Introduction to the model

According to the literature review, QoS performance of IoMT devices is decreased by the use of complicated encryption methods in current security models for IoT-based healthcare installations. Their real-time usefulness for applications like in-patient monitoring and therapy is consequently reduced. This section suggests developing a QoS-aware sidechaining paradigm that can be applied in massively scaled healthcare deployments to get around this restriction. A Novel Machine Learning Model (MLM) that splits the primary blockchain into numerous shards using a Genetic Algorithm will be used to complete this operation. These shards ensure low latency and great communication throughput by incorporating QoS-awareness into the scheme. Figure 5.1 depicts the whole model flow. It demonstrates how the chains can be split and combined using the interactive Q-Learning (IQL) technique to manipulate the shards (or sidechains). Depending on the temporal utility of the sidechains, combination or archiving operations are carried out on them. While splitting operations are carried out based on the network deployment's current QoS performance. Consequently, the IQL Model aims to gradually increase QoS awareness while lowering the chance of attack for different request types, whereas the GA Model combines improved security with higher QoS levels for healthcare installations. Each of these modules is covered in its own section of this page. The design of the complete model is broken down into a number of smaller modules.

5.2.1. Healthcare Deployments for Security and Quality of Service using GA Model

A GA-based model that examines the state of the blockchain and chooses a sidechain for storage handles all requests for data storage. Table 5.1 shows the block structure that was used for this purpose,

Table 5.1 Block structure used for storing patient data

Previous Hash	**Sensor Details**	**Sensor Values**	**Patient Details**	**Timestamp**
Doctor Information	Sidechain Number	Metadata for sidechains	Nonce	Current Hash

The following data is shown in this graphic to show that each block contains it:,

- The hash of the preceding block, which contains features for transparency and traceability
- Sensor information and sensor value, which help identify the type of sensor, the measured value, and other sensor-specific factors.

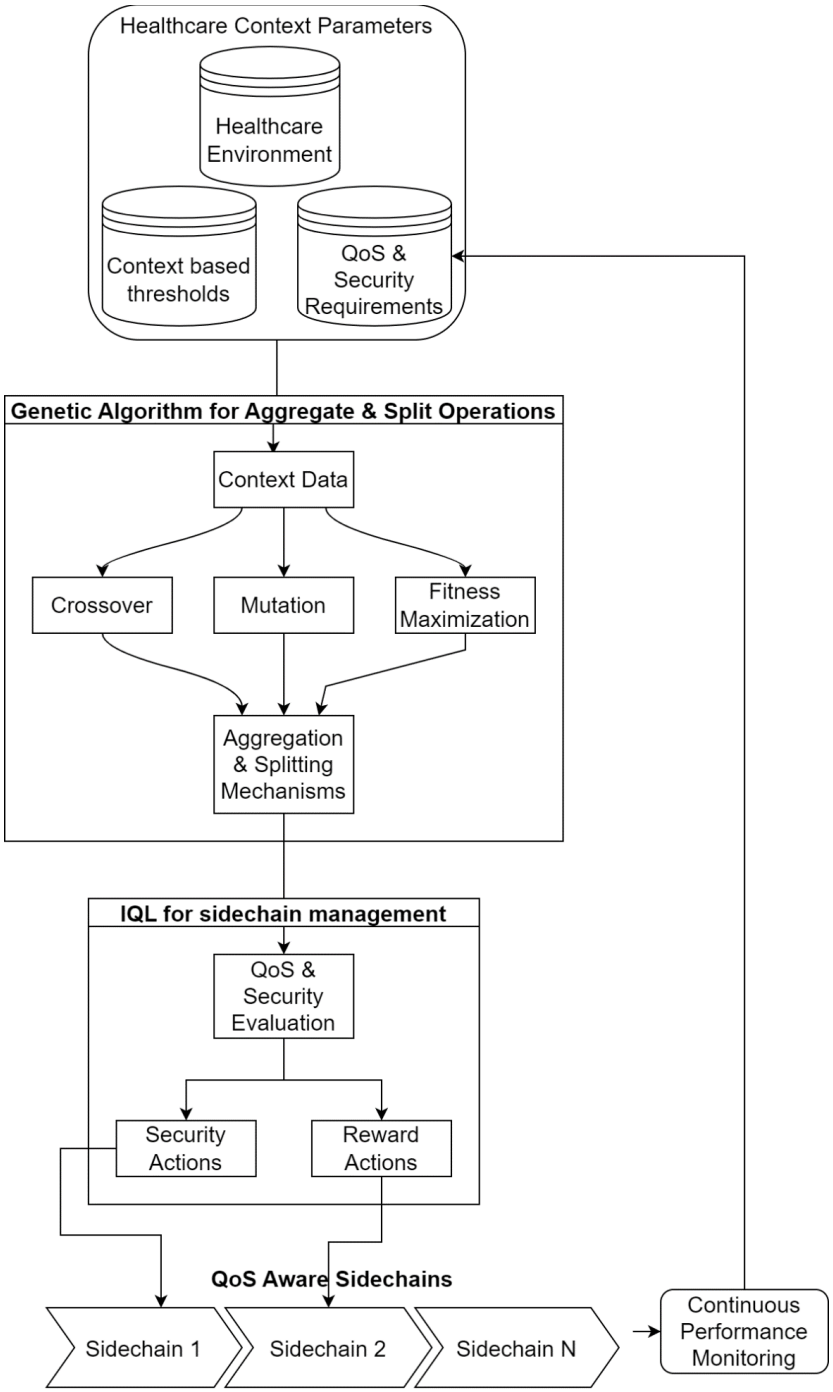


Figure 5.1. Overall flow of the proposed model

- Patient information, such as Name, Address, and Contact Information, which can be used to identify patients specifically.

- Timestamps keep track of the present time for temporal analysis.
- Doctor Detail, which can be used to identify a doctor by name, address, specialty, contact information, etc.
- Sidechain Number, which separates the current sidechain from a number of other chains and is composed of sidechain ID.
- Sidechain Information regarding the sidechain, such as the amount of blocks and aggregation criteria, are stored in meta data.
- To identify blockchain hashes, once is a random number that is used in a certain way.
- The most recent block's hash is stored in Current Hash, which is used in deployed blockchains to implement immutability.

The Proof of Work (PoW) consensus algorithm is used to process each request for a block addition, which helps to streamline the mining procedure. The PoW Model necessitates the examination of distinct hashes that adhere to a predetermined set of principles. In order to reduce the time needed for mining operations, the suggested GA Each batch of N_batch block addition requests results in an evaluation of the model. The model can function thanks to the following activities:

- Initialize the following GA Parameters,
    - Overall Number of validation iterations to be used (N_i)
    - The total number of solutions for optimisation (N_s)
    - Rate of learning for selecting crossover and mutation procedures (L_r)
    - Number of sidechains at present (N_{sc})
    - Each sidechain's length (L_{sc})
- Initialise all solutions with "to be mutated"
- For every cycle, complete the following tasks between 1 to N_i,
    - Follow these steps to assess sidechains for each solution between 1 to N_s,
        - If the current solution is marked as "not to be mutated," move on to the next entry in the list.
        - Otherwise, create a new solution using the next procedure.,
- Use equation 5.1 to select a sidechain at random,

$$Sel_{sc} = STOCH(1, N_{sc}) \quad (5.1)$$

Where, Sel_{sc} represents a chosen sidechain, and STOCH produces a random number within the given ranges.

- After adding the current blocks to this sidechain, use equation 5.2 to assess its fitness,

$$f_i = \frac{L_{sc}}{Max(\cup L_{sc}) * N_{batch}} \sum_{j=1}^{N_{batch}} \frac{D_j}{Max(D)} + \frac{E_j}{Max(E)} + \frac{Max(T)}{T_j} + \frac{100}{PDR_i} \quad (5.2)$$

Where, $D, E, PDR, \& T$ stands for end-to-end delay, energy consumption, packet delivery ratio, and throughput, which is calculated by equations 5.3, 5.4, 5.5 and 5.6 as follows,

$$D = t_{end} - t_{start} \quad (5.3)$$

$$E = RE_{start} - RE_{end} \quad (5.4)$$

$$T = \frac{P_{rx}}{D} \quad (5.5)$$

$$PDR = \frac{P_{rx}}{P_{tx}} \quad (5.6)$$

Where, t_{end} & t_{start} illustrates block addition requests' completing and starting timestamps, whereas RE, P_rx, and P_tx show the amount of energy that is still available after a block addition request has been completed.

- Using this assessment, fitness levels are computed for various solutions.
- Repeat this process for each solution, and use equation 5.7 to get the iteration fitness threshold,

$$f_{th} = \sum_{i=1}^{N_s} f_i * \frac{L_r}{N_s} \quad (5.7)$$

  - Mark the answer as "to be mutated" or if $f_i \geq f_{th}$, else mark it as ‘not to be mutated’

- Use this procedure throughout all iterations

Find the least fit solution at the conclusion of the previous iteration and choose it as a likely candidate for the addition of blocks. Run Sybil, Man in the Middle, and Distributed Denial of Service (DDoS) attacks on the chosen chain now to evaluate its resilience. Consider the following approach based on the fitness levels you've learned,

- If $f_{attack} \leq \frac{f_{normal}}{L_r}$, The blockchain can then be used without split or aggregation methods because its security performance is good.
- Else, the following procedure is used to either separate or combine blockchain with other chains,
  - If $f_{attack} \geq \frac{f_{normal}}{2 * L_r}$, then divide the blockchain into two equal sections and add blocks of shorter duration to the chain.

- Else, combine the current sidechain with a sidechain of a shorter length, then add blocks using this lengthy chain.

Blocks are added using this technique to sidechains that already exist, new sidechains of a smaller length, or aggregated sidechains of a larger length, which helps to improve QoS & security performance in a variety of real-time network deployments. Utilizing an IQL Model, which continuously assesses the security and QoS settings in situ and determines whether to split or combine the chains, improves performance even further. The paragraph that follows goes into further depth about this model's design.

5.2.2. Design of the IQL Model to maintain outstanding security performance while gradually enhancing QoS-awareness

For ongoing performance, an IQL Model is used & QoS monitoring after adding a block to a selected sidechain, which enhances its real-time deployment capabilities. Equation 5.8, which is produced for requests for successive block additions, is used by the system to evaluate a reward function. It uses fitness scores from the GA Model to continuously improve performance,

$$r = \frac{f(New) - f(Old)}{\partial} - \emptyset * Max[\cup f] + f(Old) \qquad (5.8)$$

Where, $f(New)$ & $f(Old)$ represents new and old fitness values, whereas the model's learning rate and the discount factor, which aid in ongoing QoS performance optimisation. The present sidechain configuration is split into two pieces and uses the smaller sidechain for block addition if the value of r>1, which indicates that QoS levels are decreasing. Other than that, the current configuration is ideal and doesn't call for any split procedures. As a result, the model has an enhanced security performance, high PDR, low energy consumption, and high throughput. In the following part, The model's real-time deployment capabilities are demonstrated by evaluating and comparing its performance to other state-of-the-art models.

5.3 Result & Comparisons

The research has shown that the QSIH paradigm integrates quality of service awareness with security awareness for a variety of specific real-time use cases. As a result of the model's preparation for Sybil, DDoS, and MITM attacks, it can lessen the impact of these assaults in a variety of hospital management settings. The commonly used blockchain-based healthcare deployments reported in LSR DM EH [35], LCDL [42], and BEC [48] were compared to the accepted QSIH model in order to assess the veracity of these claims.

These medical facilities are put through a range of tests under various conditions and dangers in order to give a reliable evaluation of how well they function. Throughout each iteration, the same nodes—with a linear range of 500 to 5000 patient-to-doctor exchanges—were employed for communication. This was achieved with standard network configurations. To assess how well the security system defended against Sybil, Distributed Denial of Service (DDoS), and Man in the Middle (MITM) attack types, the likelihood of attacker nodes was raised from 5% to 25%. Typical quality of service levels were assessed and tested during these attacks in terms of energy expenditure (E), packet delivery ratio (PDR), throughput (T), and from end to end communication delay (D). The following elements are taken into account in connection to this performance: We examine QoS performance under assault in section 5.2, which aids in determining QoS values for different network topologies. Part 5.1 examines QoS performance in the absence of any attacks.

5.3.1. Performance of QoS for diverse deployments in healthcare

Performance-wise, the suggested QSIH model outperforms the LSR DM EH [35], LCDL [42], and BEC [48] models. Consequently, trust-based routing incorporates QoS knowledge. This degree of performance is evaluated by treating 500 patients instead of 100, and by calculating the QoS values for different patient-to-doctor communication volumes (NPTDC). To approximate the final quality of service values, each transmission's network characteristics are simulated, and the results are combined. With the help of this averaging technique, it is feasible to precisely assess the performance of the underlying model and compare this model's performance to that of other popular models in safe hospitals. Table 5.2 displays the end-to-end delay (D) findings for patients 100, 250, and 500 in the following manner,

Table 5.2 Average end-to-end delay for various blockchain communication

No.	**Of**	**Patients**		
NPTDC	**D (ms) LSR DM EH [35]**	**D (ms) LCDL [42]**	**D (ms) BEC [48]**	**D (ms) QSIH**
500	0.90	1.01	1.10	0.79
600	0.97	1.08	1.18	0.84
700	1.03	1.14	1.24	0.89
800	1.07	1.20	1.30	0.93

900	1.13	1.26	1.39	1.00
1000	1.20	1.40	1.58	1.16
1250	1.36	1.72	1.96	1.45
1500	1.78	2.19	2.46	1.80
2000	2.23	2.64	2.90	2.10
2250	2.60	2.95	3.24	2.34
2500	2.81	3.26	3.59	2.60
2750	3.16	3.67	4.03	2.92
3000	3.55	4.10	4.52	3.27
3500	3.96	4.65	5.09	3.59
4000	4.09	4.87	5.36	3.77
5000	4.22	5.09	5.56	3.89

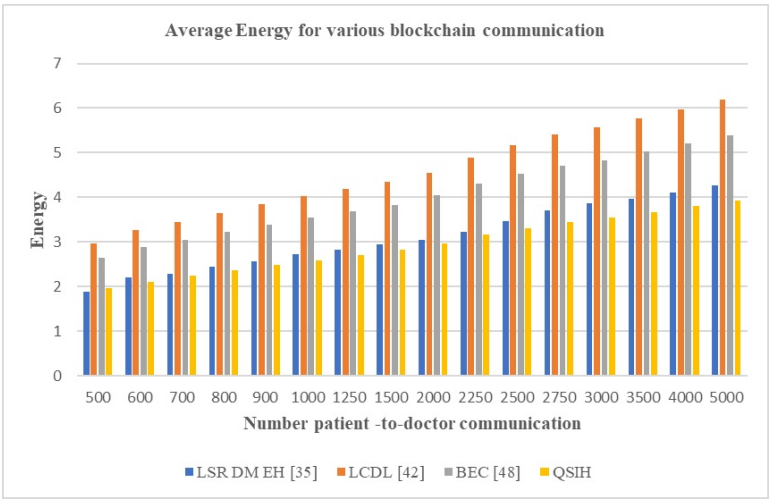


Figure 5.2 Average end-to-end delay for various blockchain communication

This analysis and figure 5.1 show that the suggested model's latency is 18.5 points lower than BEC [48], 15.5 points lower than LCDL [42], and 10.4% lower than LSR DM EH [35]. This is as a result of the model's generation using delay-aware mining techniques. These initiatives help to improve the quality-of-service requirements for the system model, which in turn improves the system's overall performance in a range of deployment circumstances. Regarding the patients' energy performance, similar findings are made, and table 3 displays the total outcomes for 100, 250, and 500 patients,

Table 5.3 Average energy for various blockchain communication

No. of Patients 100, 250, 500				
NPTDC	**E (mJ) LSR DM EH [35]**	**E (mJ) LCDL [42]**	**E (mJ) BEC [48]**	**E (mJ) QSIH**
500	1.89	2.97	2.655	1.962
600	2.205	3.267	2.88	2.115
700	2.286	3.438	3.042	2.241
800	2.448	3.645	3.222	2.367
900	2.574	3.852	3.393	2.484
1000	2.718	4.032	3.537	2.592
1250	2.826	4.194	3.681	2.7
1500	2.943	4.347	3.825	2.817
2000	3.042	4.554	4.041	2.97
2250	3.222	4.878	4.311	3.168
2500	3.474	5.166	4.527	3.312
2750	3.699	5.409	4.707	3.438
3000	3.861	5.562	4.833	3.537
3500	3.96	5.76	5.022	3.672
4000	4.113	5.976	5.202	3.807
5000	4.275	6.183	5.382	3.933

The suggested model uses 4.9% less energy than the LSR DM EH [35], 10.5% less energy than the LCDL [42], and 8.3% less energy than the BEC [48] because energy-aware mining and sidechain selection algorithms are used. This evaluation, as well as figure 5.3.2, which shows that the suggested model has these numbers under various circumstances, can be used to show this. The outcomes for 100, 250, and 500 patients are provided in table 5.2 in the manners that are shown in figure 5.2.

Figure 5.3 Average energy for various block chain communication

This contributes to raising the system model's quality-of-service levels, which in turn raises the model's overall performance across a range of deployment scenarios.

Comparable conclusions are drawn about throughput performance, which are pooled for 100, 250, and 500 patients and displayed in table 5.4,

Table 5.4. Average throughput for various block chain communications

No. of Patients				**100, 250, 500**
NPTDC	**T (kbps) LSR DM EH [35]**	**T (kbps) LCDL [42]**	**T (kbps) BEC [48]**	**T (kbps) QSIH**
500	258.624	269.955	312.21	314.757
600	261.045	272.115	314.64	317.214
700	262.746	274.149	317.07	319.77
800	264.924	276.57	319.86	322.614
900	267.417	279.027	322.695	325.422
1000	269.676	281.358	325.44	328.149
1250	271.935	283.698	328.194	330.867
1500	274.194	286.029	330.894	333.594
2000	276.444	288.36	333.594	336.312
2250	278.703	290.691	336.294	339.03
2500	280.962	293.067	338.994	341.757
2750	283.221	295.443	341.694	344.475
3000	285.48	297.819	344.394	347.202
3500	287.73	300.114	347.067	349.893
4000	289.989	302.409	349.74	352.584
5000	292.248	304.704	352.413	355.266

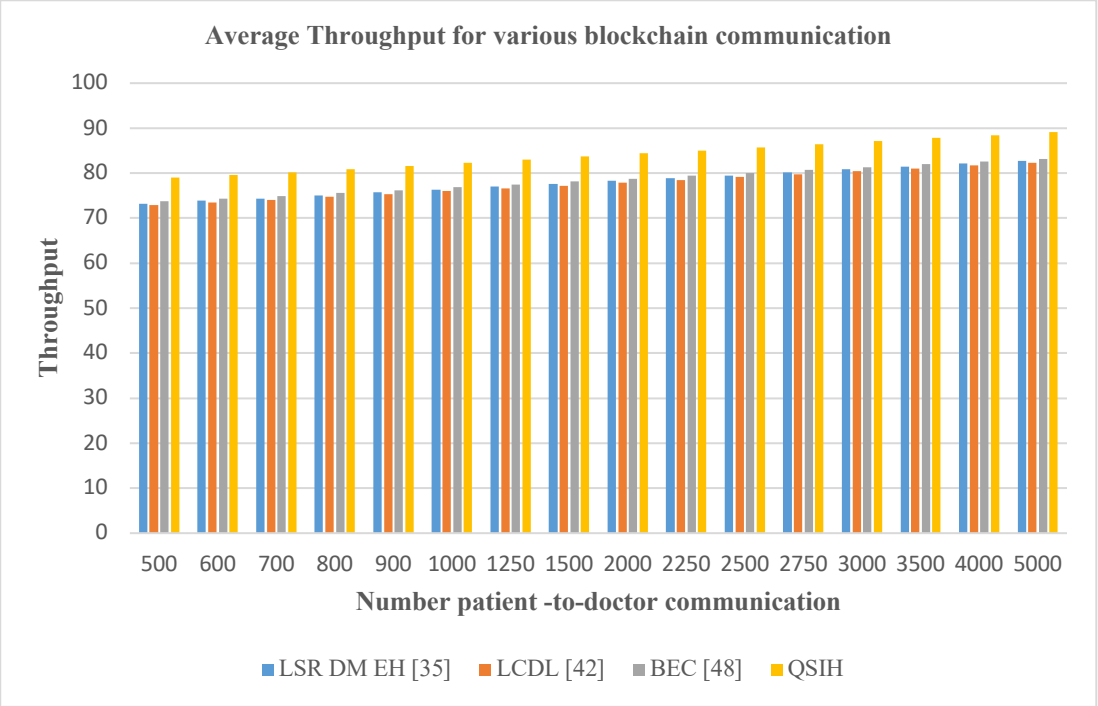


Figure 5.4. Average throughput for various blockchain communications

Throughput is 25.5% greater than LSR DM EH [6, 23.8% higher than LCDL [42], and 19.5% higher than BEC [48] when mining and sidechain selection throughput are included. This analysis and Figure 5.3 make it clear that the proposed model is more capable than LSR DM EH [35]. As a result, the proposed model's quality-of-service levels are raised, improving the model's overall performance under various deployment scenarios. Similar findings have been reported on the packet delivery ratio's (PDR) performance. The aggregate findings of these observations for 100, 250, and 500 patients are displayed in table 5.5 and include the following information:

Table 5.5. Average PDR for various blockchain communications

No.	**of**	**Patients**		**100, 250, 500**
NPTDC	**PDR (%) LSR DM EH [35]**	**PDR (%) LCDL [42]**	**PDR (%) BEC [48]**	**PDR (%) QSIH**
500	73.206	72.9	73.728	78.984
600	73.89	73.485	74.304	79.596
700	74.376	74.025	74.88	80.235
800	74.997	74.691	75.546	80.946

900	75.699	75.357	76.212	81.648
1000	76.338	75.978	76.842	82.332
1250	76.977	76.617	77.481	83.016
1500	77.616	77.247	78.12	83.7
2000	78.255	77.886	78.768	84.384
2250	78.894	78.516	79.398	85.068
2500	79.524	79.155	80.046	85.752
2750	80.172	79.785	80.685	86.436
3000	80.811	80.415	81.315	87.12
3500	81.45	81.054	81.954	87.813
4000	82.089	81.675	82.593	88.488
5000	82.728	82.305	83.223	89.163

The PDR of the proposed model is 6.5% higher than LSR DM EH [6, 5.9% higher than LCDL [42], and 4.5% higher than BEC [48] as a result of PDR being included for mining and sidechain selection activities. Figure 5.4 and this assessment can be used to demonstrate how, in different scenarios, the PDR for the system model is significantly greater.

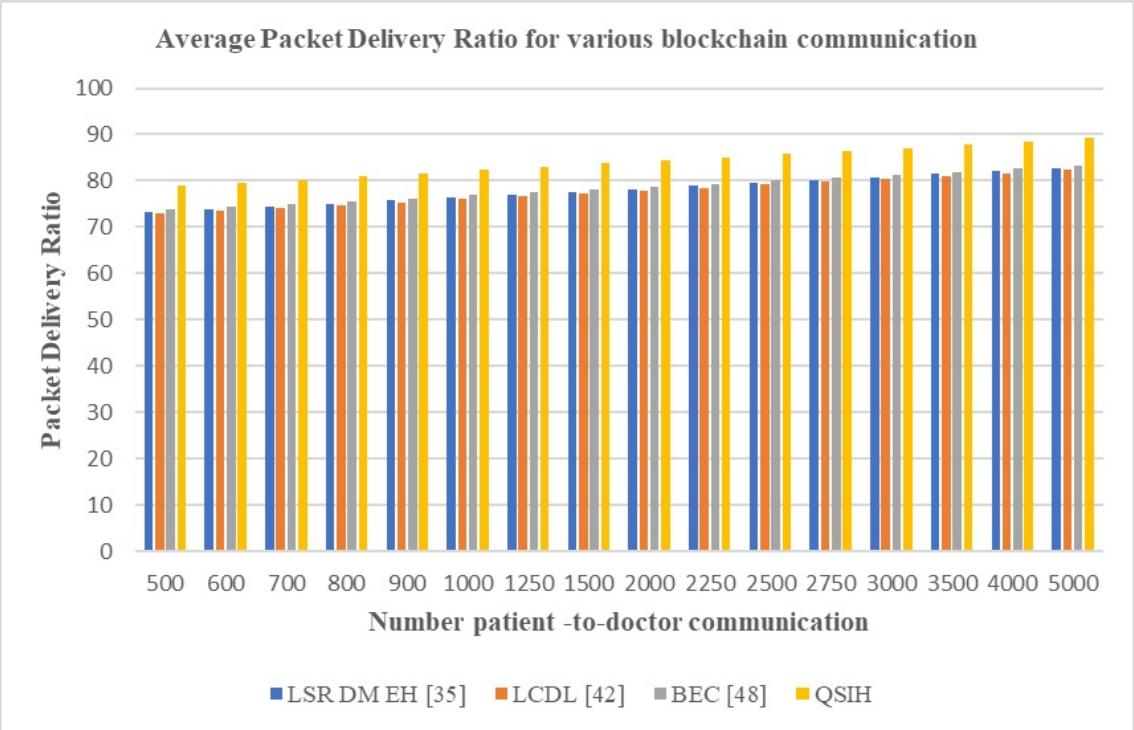


Figure 5.5 Average PDR for various blockchain communications

This helps to raise the suggested model's quality-of-service levels, which ultimately improves the model's overall performance under various deployment scenarios. These evaluations are expanded to account for a range of shifting attack quantities within the network in the section that follows.

5.3.2. Security outcomes for various healthcare models under network assaults

By merging IQL with GA-based blockchain technology, the suggested model for data communications outperforms the LSR DM EH [35], LCDL [42], and BEC [48] models in terms of QoS under various attacks. The proposed solution integrates the blockchain paradigm based on GA with IQL for data transmission, which is why. The performance of this network is assessed by raising the number of attacker (NA) nodes from 5% to 25% and analysing the quality of service parameters. For Sybil, MITM, and DDoS attacks, estimates of the normal QoS values have been made. Table 5.6 lists the end-to-end delay (D) values for the various protocols used during these assaults,

Table 5.6 Average end-to-end delay for various attacks

Type of Attack Sybil, MITM, DDoS				
NA (%)	**D (ms) LSR DM EH [35]**	**D (ms) LCDL [42]**	**D (ms) BEC [48]**	**D (ms) QSIH**
5.00	0.873	0.954	0.927	0.738
5.50	0.927	1.017	0.981	0.783
6.00	0.981	1.071	1.026	0.828
6.25	1.026	1.125	1.098	0.882
10.00	1.098	1.233	1.224	0.963
12.50	1.224	1.44	1.458	1.116
13.75	1.494	1.791	1.809	1.377
15.00	1.89	2.196	2.178	1.692
16.25	2.268	2.547	2.502	1.98
17.50	2.556	2.844	2.79	2.214
18.75	2.808	3.168	3.114	2.457
20.00	3.159	3.555	3.492	2.754
21.25	3.546	3.978	3.906	3.087
22.50	3.96	4.41	4.284	3.42
23.75	4.149	4.626	4.5	3.582

25.00	4.302	4.788	4.653	3.708

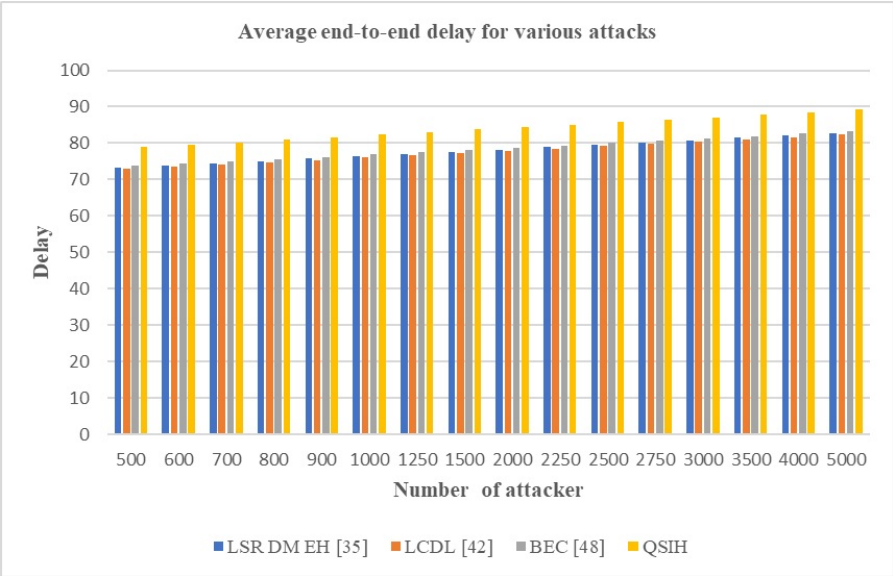


Figure 5.6 Average end-to-end delay for various attacks

We can demonstrate that the proposed model has a latency that is 15.5% less than LSR DM EH [6, 18.3% less than LCDL [42], and 16.5% less than BEC [48] using this analysis and figure 5.5. This is required in order for the proposed model to account for the time constraints imposed by sidechain selection and mining activities. This improvement in delay performance shows how the system model can maintain QoS under many attack scenarios, granting it the ability to withstand a wide range of network attacks. Concluding remarks on energy efficacy are similar. Table 5.6 shows how this can be viewed for DDoS, MITM, and Sybil attacks and has the following formatting,

Table 5.7. Average energy consumption for different attacks

Type of Attack Sybil, MITM, DDoS				
NA (%)	**E (mJ) LSR DM EH [35]**	**E (mJ) LCDL [42]**	**E (mJ) BEC [48]**	**E (mJ) QSIH**
5.00	2.403	2.682	2.61	1.881
5.50	2.655	2.889	2.799	2.043
6.00	2.799	3.06	2.952	2.151
6.25	2.97	3.231	3.114	2.277
10.00	3.132	3.393	3.267	2.394

12.50	3.276	3.537	3.402	2.502
13.75	3.402	3.681	3.546	2.601
15.00	3.537	3.843	3.717	2.718
16.25	3.708	4.068	3.942	2.862
17.50	3.96	4.32	4.167	3.042
18.75	4.275	4.59	4.374	3.24
20.00	4.545	4.851	4.59	3.429
21.25	4.833	5.112	4.806	3.618
22.50	5.112	5.373	5.022	3.807
23.75	5.4	5.634	5.238	3.996
25.00	5.679	5.895	5.454	4.185

The system model uses 16.5% less energy than the LSR DM EH [35], 18.5% less energy than the LCDL [42], and 18.3% less energy than the BEC [48] due to energy being spent during mining and sidechain selection. This analysis and Figure 5.7 demonstrate that the system model consumes 18.5% less energy than the BEC [48].

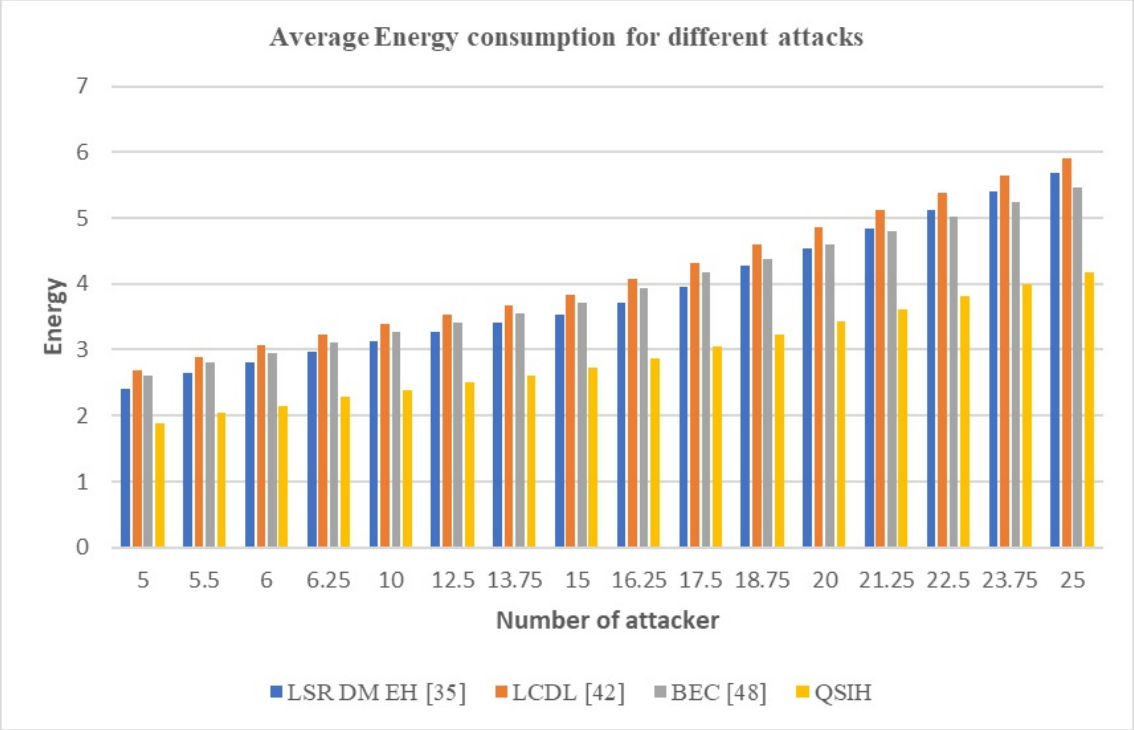


Figure 5.7 Average energy consumption for various attacks

This improvement in energy consumption performance shows that the suggested strategy may continue to deliver higher quality of service (QoS) in a variety of attack situations and is resistant to different types of network attacks. To find comparable conclusions

about throughput performance for Sybil, MITM, and DDoS attacks, look at table 5.8, which is presented as follows.

Table 5.8. Average throughput performance for various attacks

Type of Attack Sybil, MITM, DDoS				
NA (%)	**T (kbps) LSR DM EH [35]**	**T (kbps) LCDL [42]**	**T (kbps) BEC [48]**	**T (kbps) QSIH**
5.00	281.421	299.691	286.29	389.817
5.50	283.725	302.04	288.549	392.922
6.00	285.84	304.479	290.934	396.036
6.25	288.324	307.17	293.49	399.528
10.00	290.907	309.834	296.019	403.02
12.50	293.355	312.426	298.494	406.395
13.75	295.803	315.018	300.96	409.761
15.00	298.242	317.61	303.435	413.136
16.25	300.69	320.202	305.901	416.511
17.50	303.129	322.794	308.376	419.886
18.75	305.577	325.386	310.842	423.252
20.00	308.016	327.987	312.651	426.33
21.25	310.437	330.543	314.91	429.588
22.50	312.849	333.099	317.142	432.819
23.75	315.252	335.655	320.022	436.338
25.00	317.718	338.292	322.443	439.722

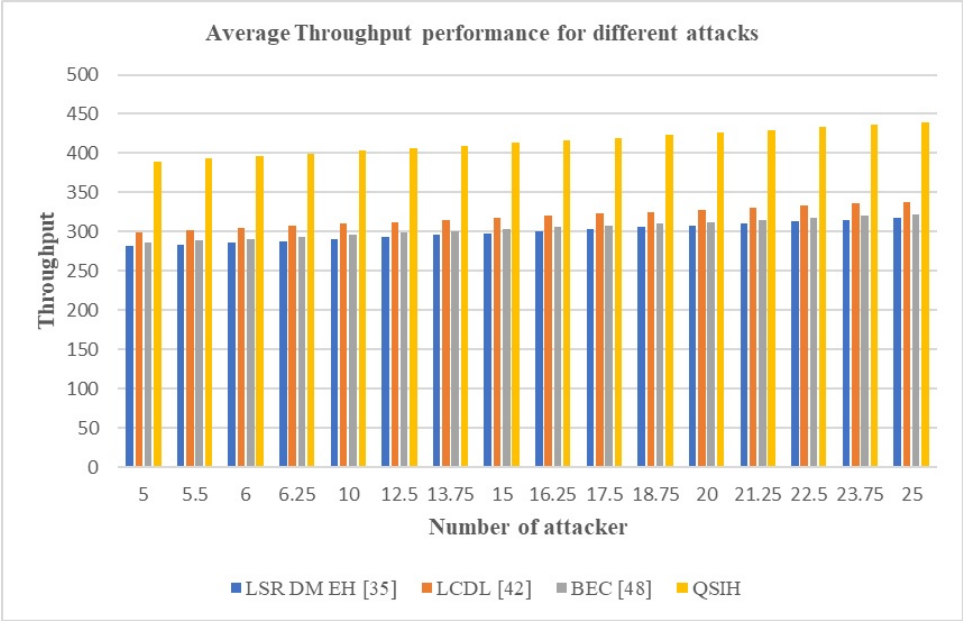


Figure 5.8. Average throughput performance for different attacks

The evaluation in figure 5.8 demonstrates that the suggested model's throughput is 16.5% greater than BEC [48] as a result of the incorporation of throughput during mining and sidechain selection procedures. Additionally, the system model's throughput surpasses LCDL [35] by 20.4%, LSR DM EH [35] by 18.3%, and LCDL [42] by much more. This increase in throughput performance demonstrates how the recommended model might improve QoS even when exposed to diverse attack types, providing it the advantage of being resistant to varied network attacks. Similar results about PDR performance have been found; table 5.9, which has the following formatting, can be used to show this for Sybil, MITM, and DDoS attacks,

Table 5.9. Average packet delivery ratio performance for various attack

Type of Attack Sybil, MITM, DDoS				
NA (%)	**PDR (%) LSR DM EH [35]**	**PDR (%) LCDL [42]**	**PDR (%) BEC [48]**	**PDR (%) QSIH**
5.00	55.647	53.361	58.581	80.856
5.50	56.169	53.784	59.04	81.486
6.00	56.538	54.18	59.499	82.134
6.25	57.006	54.666	60.021	82.863
10.00	57.546	55.152	60.552	83.592
12.50	58.032	55.611	61.065	84.285
13.75	58.518	56.079	61.578	84.987
15.00	59.004	56.538	62.082	85.689
16.25	59.481	57.006	62.586	86.391
17.50	59.967	57.465	63.09	87.084
18.75	60.453	57.933	63.603	87.786
20.00	60.948	58.392	64.107	88.488
21.25	61.434	58.86	64.62	89.19
22.50	61.92	59.328	65.133	89.892
23.75	62.406	59.778	65.637	89.901
25.00	62.883	60.237	66.132	89.955

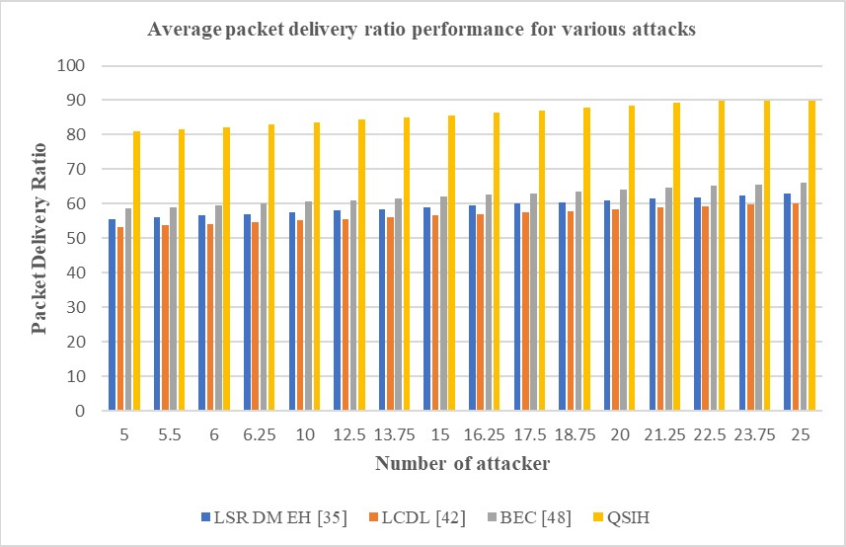


Figure 5.9 Average packet delivery ratio performance for various attacks

The system model has a PDR that is 25.5% greater than LSR DM EH [6, 28.3% higher than LCDL [42], and 23.5% higher than BEC [48] because PDR was used during the mining and sidechain selection operations. This analysis and Figure 5.9 make it abundantly evident that the proposed model has a higher PDR than LSR DM EH [35]. This increase in PDR performance shows how the proposed model may enhance QoS even in the face of various attack kinds, giving it the benefit of being resistant to various network attacks. Consequently, the proposed model achieves exceptionally high QoS, which facilitates its deployment for a range of secure healthcare applications.

5.4 Conclusion

The system approach interactively combines the IQL and Genetic Algorithm (GA) to incorporate knowledge of QoS and security. As a result, when exposed to network hazards, the model performs better in terms of latency, energy usage, throughput, and PDR. The model combines the GA Model, which offers an estimate of the various sidechain configurations, with the IQL Method, which helps the underlying blockchains scale dynamically. The IQL Method offers incentive functions following a temporal quality of service analysis on several block batches. We evaluate the incremental values of these functions and derive conclusions regarding the processes of chain aggregation, splitting, and growth. The latency of the suggested model is reduced by these integrations by 10.4% compared to LSR DM EH [35], 15.5% compared to LCDL [42], and 18.5% compared to BEC [48]. Energy-aware mining and sidechain selection algorithms utilize 10.5%, 8.3%, and 8.3% less energy, respectively, than LSR DM EH [35], LCDL [42], and BEC [48]. The model's throughput is higher, too, coming in at 25.5% higher than LSR DM EH [35], 19.5% higher than BEC [48], and 23.8% higher than LCDL [13]. In comparison to LCDL [42], LCDL [35], LSR DM EH [35], and BEC [48], the model's PDR is 5.9% higher, 5.9% higher, and 6.5% higher, respectively. This is a result of the model's integration of PDR into the processes for sidechain selection and mining. This helps to improve the quality-of-service standards of the proposed model, which in turn improves the model's overall performance in various deployment scenarios. Under several sorts of attacks, it was discovered that the suggested model performed better than LSR DM EH [35], LCDL [42], and BEC [48] by 15.5%, 18.3%, and 16.5%, respectively. This performance was further validated. Because energy was taken into account at every stage of the design process, the recommended model uses 16.5% less energy than LSR DM EH [35], 18.5% less energy than LCDL [42], and 18.3% less energy than BEC [48].

The suggested model offers the benefit of resilience to different network assaults due to the improvement in energy consumption performance, demonstrating that it can still achieve greater QoS even when faced with diverse attack types. These results were also constant for throughput and PDR levels, making the technique very valuable for real-time healthcare installations under various assault scenarios. For example, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and other deep learning techniques can be used in future research to improve the model's performance. Real-time datasets must be used for verification in order to accurately evaluate these models' scalability across various scenarios. Additionally, a large number of bioinspired models can be cascaded into one another by researchers to continuously improve sidechaining efficiency while taking into consideration a range of deployment-specific application scenarios.

CHAPTER 6

IoMT Data Processing Paradigm for Healthcare Deployments Using Deep Learning

6.1 Design of a highly secure IoMT data processing paradigm for healthcare deployments that is enabled by deep learning on the blockchain

Internet-of-Medical-Things (IoMT) designers' top priorities now include securing healthcare implementations. This is because IoMT deployments are always under attack by both internal and external opponents. To incorporate attack detection, researchers have observed that blockchain-based deployments are highly efficient, due to their immutability, traceability, distributed computing & transparency characteristics. But single-chained deployments cannot be scaled due to an exponential increase in computational delays. Moreover, processing efficiency of secure IoMT-based data must be enhanced, which will assist in adding robustness to these deployments. This chapter suggests designing a highly secure IoMT data processing model based on deep transfer learning that is driven by blockchain and can be utilised for multimodal healthcare deployments in order to combine these features. The Proof-of-Medical-Trust (PoMT) consensus, which is widely deployable and has built-in sidechain support for multichain use cases, is incorporated into the system approach to reduce blockchain write and read delays. The PoMT Model uses a Genetic Chain Optimization (GCO) method, that assists in segregating single chained data into sharded chains. The underlying data is classified into various disease categories using a deep transfer learning (DTL) based model that fuses a Gated Recurrent Unit (GRU), Long-Short-Term Memory (LSTM), and Recurrent Neural Networks (RNNs). The classified data is further processed via a customized 2D Convolutional Neural Network (2D CNN), that assists in identification of disease severity and progression levels via augmented analysis. The model's performance under various internal and external attack types was evaluated, and it was shown to be 10.4% quicker for mining, 6.5% faster for reading, and 9.3% more energy-efficient when compared to ordinary storage models. Additionally, it was found that the model performed 2.9% better at classifying diseases and had 3.5% better accuracy in identifying severity in clinical scenarios. Because of this, the model can be used for large-scale use cases.

6.2 Introduction to the model

The extensive use of new technologies and the development of complex data storage and management systems had a considerable impact on the collection, processing, and storage of medical data in the health care industry. Increasing connectivity throughout the healthcare ecosystem aims to promote information interchange, hence improving data management and service delivery. Adoption of intelligent medical devices is a crucial component in this trend. The discipline of IoMT (Internet of Medical Things) has attracted a lot of attention recently. IoMT is a networked architecture with security and fortified blockchains (FB) for interconnected health systems (hardware, software, and services). [1, 2, 3, 4]. Connecting devices, sensors, and patient data allows healthcare organizations to enhance clinical operations and workflow management and remotely monitor patients' health (e.g., from home). By bridging the gap between analog and digital, IoMT enables physicians to make more precise diagnoses and fine-tune treatments in record time. Despite its use in satisfying a range of healthcare ecosystem objectives, IoMT technologies present substantial privacy and security concerns [5, 6, 7, 8]. Due to the critical nature of IoMT features (handling sensitive medical data, providing life-saving operations, and the involvement of potentially untrusted devices and networks), IoMT systems must be designed to maximize integrity, authenticity, validity, and data privacy [9, 10, 11, 12]. To meet the many needs of the ecosystem, researchers use cutting-edge technologies like blockchain, AI, and the Internet of Things. This kind of technology significantly enhances healthcare delivery and transforms inefficient healthcare networks into full digital ecosystems [13, 14]. The blocks that comprise the blockchain constitute a peer-to-peer, decentralized network. A ledger is often used as a synonym for the distributed database technology that supports it via Neural Trust Mechanisms (NTM) [15, 16] due to the fact that it records all network transactions ever conducted. Due to the interrelated structure of transactions inside blocks, all blockchain-based operations are accurately recorded and timestamped. As a result, users are confined to reading and uploading data in accordance with the restrictions specified by the network's stakeholders, and cannot modify any stored information. It is up to the various network participants to evaluate if transactions are valid and should be preserved [17, 18, 19, 20]. Thus, consensus procedures are used, which, depending on the application situation, may or may not be advantageous. The two most popular methods are Proof-of-Work (PoW) and Proof-of-Stake (PoS) . One of the several distinct consensus methods for blockchain

networks that can keep working even in the event of a node's failure or malicious activity is Proof-of-Medical-Trust (PoMT). In blockchain applications, the use of smart contracts (SC) may be seen as the digital version of conventional contracts. SCs are blockchain-based, self-executing programs that execute the terms of an agreement when specific criteria are fulfilled [21, 22, 23]; The system executes each transaction utilizing SCs without the need for middlemen under different use cases via Inter Planetary Health Layer (IPHL) designs [24, 25].

The Internet of Medical Things has significantly facilitated access to medical services by becoming a fundamental part of peoples' daily lives as a result of information technology advancements. Using smart terminals, patients may take care of a range of healthcare requirements, including registration, without visiting a hospital. The patients realize considerable cost and time savings. Despite the ease of electronic medical services, the widespread use of IoMT devices exposes patients to network vulnerabilities and privacy breaches that also include deep learning (DL) models [26, 27, 28, 29]. In light of this, privacy protection has become a crucial concern for IoMT. According to work in [30, 31, 32], authentication techniques are often used to construct a system of stringent privacy protection. User authentication in IoMT necessitates a complex method of data transfer between the user and other servers. People often think that workers in the service profession are usually honest, dependable, and inquisitive [33]. In a centralized client-server approach, patient authentication is conceivable, however this model has several security and privacy issues. [34, 35]. An important research challenge is how to effectively authenticate patients with medical servers while safeguarding their privacy. To guarantee patient anonymity in an IoMT environment where patient devices have limited processing capacity, a lightweight authentication approach is required. Numerous authentication strategies have been presented by academics [36, 37, 38], but it may be challenging to achieve an appropriate balance between authenticity and computational complexity. In general, they are neither dependable nor secure. In recent years, blockchain research has become more popular. Blockchain-assisted technology presents a viable solution for authentication schemes utilising Attention-Based Multilevel Co-Occurrence Graph Convolutional LSTM (ABM CGC LSTM), particularly in the healthcare industry, the internet of cars, the smart grid, etc. [39, 40, 41].

The Internet of Medical Things (IoMT), a rapidly expanding subset of Internet of Things (IoT) applications, uses medical devices to provide a range of healthcare solutions. The healthcare sector has improved thanks to digital technologies. IoMT-based healthcare

systems have the potential to improve quality of life, save costs, and increase patient awareness. From the perspective of the healthcare provider, the IoMT may minimize device interruptions by utilizing remote provisioning. The IoMT can also pinpoint with accuracy when it is advisable to replace supplies in order to maintain the functionality of a range of devices. It enables the IoMT to deliver cutting-edge patient services while making the most use of scarce resources. Internet of Medical Things wearable gadgets collect a range of private data when their owners carry them in their pockets. This knowledge can help carers and medical professionals decide on a patient's treatment in a timely, evidence-based manner. In contrast, this information is very private and secret.

It is the user's responsibility to take appropriate security and privacy measures for their personal health information. IoT privacy and security are two major issues. Internet of Things (IoT) devices are unable to meet the stringent resource requirements of traditional security solutions because of the limited availability of these resources. The cloud enables an increasing number of Internet of Things (IoT) applications by providing infrastructure and capabilities to devices with limited resources. Due to the limited processing and storage capacity of internet-of-things devices [42], a cloud layer is necessary to meet the increased demand. In addition, standard security methods are useless against IoT devices [43]. The internet of medical things (IoMT) makes use of mobile phones and other technologies to enhance an individual's health. However, IoMT's scientific potential is what makes it so interesting. Using medical technology, it may be possible to identify new illnesses and remedies. For instance, the general public may create a worldwide dataset that contains each unique clinical account [44].

In the absence of a trustworthy context, failing to take precautions against risks, such as forgetting to encrypt private medical data, is an example of what might happen in an untrustworthy setting. Individual and patient-centred care is denoted by the abbreviation IoMT, which refers to the capacity of patients to control their own prescription regimens, keep their own health records, and electronically exchange pertinent information with their physicians. Modern encryption software is used by the BCT to address security concerns with the IoMT. Cloud computing is one of the most discussed research topics because of its vast resource sharing potential and enhanced user interface [45]. Proportionate Data Analytics (PDA) is helping cloud computing gain more traction in response to the need for scalable and efficient service delivery [46]. Internet-delivered computer services such as servers, networking, databases, software, and data analytics allow for faster deployment, more flexible use of resources, and cheaper per-user prices

because of economies of scale. In some situations, we use the phrase "cloud computing" to characterize this strategy. Cloud computing has enormous economic potential and is increasing rapidly. However, cloud storage solutions have serious security and trust difficulties. Additionally, in 2019, the data of 10.6 million MGM Resorts customers was stolen owing to a cloud server flaw that was covered via use of convolutional neural network with recursive neural network (RCNN). [101]. In 2016, at least 2 million websites were impacted by a Cloudflare infrastructure flaw that exposed encrypted client data [10]. Businesses using alternative public cloud storage services were badly affected by Microsoft Azure issues for more than eight hours. In June 2017, a data breach affecting Amazon Web Services [10] revealed sensitive voter information. According to a survey conducted in 2020 by Check Point Inc., 82% of users think that current security measures are insufficient to fend off cloud security issues, and 52% think that the public cloud is more vulnerable to attacks than the traditional environment [48]. These concerns and findings indicate a lack of user confidence in the cloud environment as well as basic issues with trust management, even though cloud computing has come a long way. Numerous scholars have examined the difficulties of managing trust in cloud computing. Work in [49] have created a paradigm-shifting approach to trust that enables users to study and predict their own cognitive processes. In addition to trust models and evolutionary algorithms [50], a variety of practical ways for managing trust-enabled systems have been presented. In contrast, the old trust paradigm's reliance on a single point of failure and a central trust control centre for third parties could cause delays and traffic jams. Users are permitted to independently verify the assessment's findings because not all users in a centralised trust system have access to the proof of trust. A hospital's medical records may be uploaded to the cloud for storage and later review by authorised people. With cloud-based IoMT, there are immediate security, privacy, and trust concerns. Recently, researchers have shown a growing interest in security, privacy, and trust. Protection of sensitive data guarantees its accuracy, authenticity, and, most importantly, its integrity. In addition, it controls information access to approved parties. When designing IoMT, it is essential to consider privacy. It understands the importance and sensitivity of information sent across an open channel. Context and content are required for the maintenance of privacy. Protecting the anonymity of a patient is challenging since an attacker may learn a great deal about the patient's condition simply discovering the identity of the treating physician. Using content privacy to safeguard critical patient data. Moreover, contextual anonymity is crucial. The phrase "contextual privacy" refers to the

protection of the background information of a communication. In the medical industry, IoMT-based systems use a variety of symmetric and asymmetric encryption techniques. Recent research has shown that high-powered machine learning (ML) techniques are not the best option for low-powered devices such as IoMT. To solve this problem, complex ML algorithms should be run on IoT devices and in the cloud utilising straightforward privacy-preserving methods. On the subject of cloud-based IoMT security for healthcare systems, numerous studies have been published. Blockchain technology has several uses, including cryptocurrencies, security, managing trust, and immutability.

The system is durable in the absence of a centralised authority even when a few nodes fail. In operational rules and data documents, transparency, nonrepudiation, and secrecy may be maintained via the use of digital signatures, data chains, and consensus procedures. For the development of contemporary decentralized trust systems, the blockchain's decentralization property is vital [18]. The development of a reliable cloud computing environment using blockchain technology [19, 20]. Blockchain technology is also a workable choice in this situation for providing security, trust, and authenticity. A blockchain-based solution for managing trust has been created by many researchers to far and has attracted a lot of interest. Following this, we compared, organised, and looked at several major challenges for various applications..

Due to its immutability, traceability, distributed computing, and transparency, blockchain-based deployments are superior than conventional methods for detecting attacks, as shown by this study. However, single-chained deployments cannot be expanded due to exponentially increasing computational delays. To strengthen these infrastructures, the pace at which data based on the secure IoMT is processed must be increased. In the next part, we propose the construction of a blockchain-powered, deep transfer learning-based, and highly secure IoMT data processing model keeping these features in mind. This method is applicable for multifaceted healthcare rollouts. Section 6.3 of this paper compares the system model to different other state-of-the-art models, and then uses the comparisons to validate the new model in a variety of clinical settings. The suggested model is discussed in this work's conclusion along with some comments on it that are pertinent to the context and suggestions for how to make it better for various uses.

6.2 Design of the proposed Blockchain-powered Deep transfer learning-based highly Secure IoMT data processing model for Healthcare Deployments

Design of proposed Genetic chain Optimisation (GCO) based Sharding and Classification for Secure IoMT data Model:

Based on the work done for blockchain-based security enhancement of IoMT device deployments, it can be observed that single-chained deployments cannot be scaled due to an exponential increase in computational delays. Moreover, processing efficiency of secure IoMT-based data must be enhanced, which will assist in adding robustness to these deployments. This section suggests designing a deep transfer learning-powered blockchain-based highly secure IoMT data processing model that can be applied to multimodal healthcare installations in order to combine these features. The proposed model's architecture is depicted in Figure 6.1, where it is clear that by integrating a Proof-of-Medical-Trust (PoMT) consensus that can be implemented across numerous nodes and having built-in sidechain support for multichain use cases, the model lowers blockchain write and read delays. The PoMT Model uses a Genetic Chain Optimization (GCO) method, that assists in segregating single chained data into sharded chains.

A deep transfer learning (DTL) based model that integrates a Gated Recurrent Unit (GRU), Long-Short-Term Memory (LSTM), and Recurrent Neural Networks (RNNs) is used to classify the underlying data into different medical conditions. Data is safely kept on these sharded chains. The categorised data is then further processed using a tailored 2D Convolutional Neural Network (2D CNN), which helps identify the severity and rate of disease progression through augmented analysis. It is clear from this flow that a Proof-of-Medical Trust (PoMT) based consensus model processes all input data at the outset, helping to identify the best nodes for mining activities.

This PoMT based consensus model works as per the following process,

- For each data communication request, identify source & destination node sets

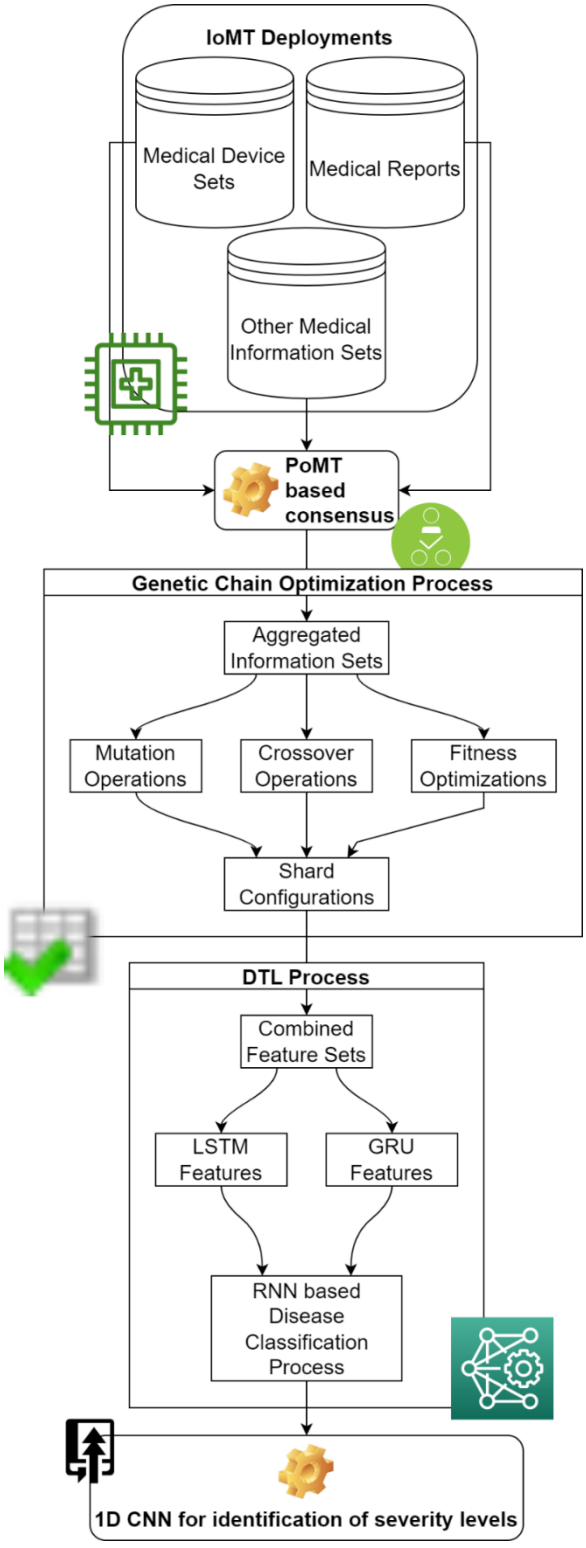


Figure 6.1. Design of the proposed GCO based sharding and classification process

- Identify all 1-hop neighbours of the source node, and estimate their Medical Trust Score (MTS) via equation 6.1,

$$MTS_j = \sum_{i=1}^{N_c} \frac{E_{i,j}}{d_{src,j}} * \frac{THR_{i,j}}{Max(THR)} * \frac{PDR_{i,j}}{100} \quad (6.1)$$

Where, $E_{i,j}$ represents energy levels of current node during i^{th} communication, $d_{src,j}$ represents distance between source & current node, THR represents its throughput levels, while PDR represents it packet delivery ratio levels for each of the previous N_c communications.

- Select node with highest value of MTS, and select it for mining purposes
- If the selected node is marked as 'N_{sel}', then evaluate MTS for all 1-hop nodes from N_{sel} that are towards the destination node, which can be ensured via equation 6.2,

$$d_{src,N_{sel}} < d_{src,dest}\ AND\ d_{dest,N_{sel}} < d_{src,dest} \quad (6.2)$$

- This process is repeated till destination node and N_{sel} are in 1-hop radius from each other, which indicates convergence of the PoMT consensus

All selected nodes are used for consensus operations, and are responsible for verification of block hashes. The same nodes are also used for communication of data between source & destination node pairs. During every communication, data is initially stored on a single blockchain, which has a format as indicated via table 6.1,

Table 6.1. Structure of the blockchain used for storage operations

Source IP	Destination IP	Hop Information	Data Samples	Timestamp
Nonce	Previous Hash	Meta Data Sets	Shard Information	Current Hash

Data is stored on the blockchain after mining operations from each of the hop nodes, and mining delay is estimated via equation 6.3,

$$d(Mining) = N * d(Read) + (N-1) * \big(d(Verify) + d(Hash)\big) + d(Write) \quad (6.3)$$

Where, $d(Mining)$ represents delay needed for mining operations, while N represents number of blocks stored on the current blockchain shard (Initially, Number of shards = 1), and $d(Read), d(Write), d(Hash)$ & $d(Verify)$ represents delays needed for reading, writing, hashing and verifying blocks. Mining delay between consecutive blocks is estimated, and its slope is evaluated via equation 6. 4,

$$S = \frac{d(Mining)_{i+1}}{d(Mining)_i} \quad (6.4)$$

If the value of this slope $S > 2$, then it indicates that delay is getting doubled for the current blockchain length, thus a Genetic Chain Optimization (GCO) based model is used to divide current chain into 2 unequal shards via the following process,

- Initially, setup following constants for optimization of the shards,
    - Total Genetic iterations needed for optimization (N_i)
    - Total Genetic solutions needed for optimization (N_s)
    - Rate at which each solution will learn from previous solutions (L_r)
- For the selected shard, generate N_s different solutions as per the following process,
    - Divide the shard into 2 shares of unequal lengths as per equation 6.5 & 6.6,

$$L_1(New) = STOCH(L_r * L, L - 1) \quad (6.5)$$

$$L_2(New) = L - L_1(New) \quad (6.6)$$

Where, $STOCH$ represents a Markovian process for generation of stochastic number sets, while L represents length of current chain which needs optimizations.

    - Select the smaller shard, and add N_i blocks to it for evaluation purposes.
    - While adding these blocks, estimate solution fitness via equation 6.7,

$$f = \frac{\sum_{i=1}^{N} S_i}{N} \quad (6.7)$$

    - Repeat this procedure for each solution to determine each person's degree of fit
- Once all solutions are generated, then estimate fitness threshold via equation 6.8,

$$f_{th} = \sum_{i=1}^{N_s} f_i * \frac{L_r}{N_r} \quad (6.8)$$

- All solutions are scanned for N_i iterations, and solutions with $f > f_{th}$ are regenerated, while other solutions are not modified during the iteration process

The solutions with the highest fitness are chosen at the end of each iteration, and the shard configurations from these solutions are used for block storage operations. As a result, the model may maintain greater throughput and PDR levels while reducing mining latency and using less energy. Figure 6.2 illustrates the use of an LSTM and GRU-based feature representation model, which integrates the two models for feature extraction and selection, to analyse data kept on these Chains.

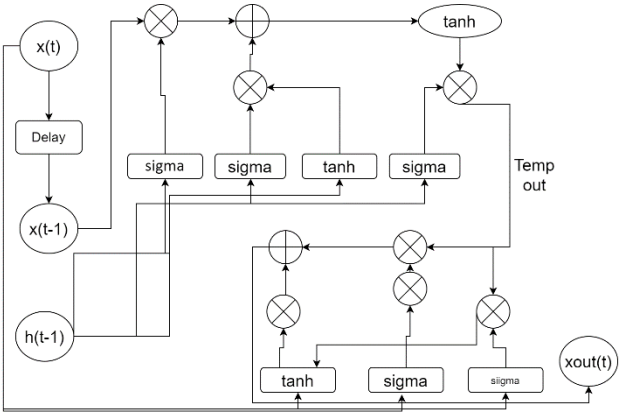


Figure 6.2. Design of the LSTM & GRU based feature extraction process

The model extracts a large set of variance-based feature sets, which assists in representing medical data into multiscale variance components. To perform this task, a set of features including initialization (i), temporal output (o), and function feature vectors is estimated via equations 6.9, 6.10 and 6.11 as follows,

$$i = var\left(x_{in} * U^{i} + h_{t-1} * W^{i}\right) \tag{6.9}$$

$$o = var(x_{in} * U^{o} + h_{t-1} * W^{o}) \tag{6.10}$$

$$f = var(x_{in} * U^{f} + h_{t-1} * W^{f}) \tag{6.11}$$

Where, U & W represents constants of the LSTM process, while var represents variance levels, and h represents contextual kernel matrix, which is initialized with class-level variance for different disease types. These features are extended via estimation of a convolutional feature vector via equation 6.12,

$$C_t' = tanh(x_{in} * U^{g} + h_{t-1} * W^{g}) \tag{6.12}$$

Similar to this a temporal feature vector is estimated via equation 6.13,

$$T_{out} = var(f_t * x_{in}(t-1) + i * C_t') \tag{6.13}$$

Based on this value, the kernel metric is updated as per equation 6.14,

$$h_{out} = \tanh(T_{out}) * o \tag{6.14}$$

The temporal feature vector T_{out}, is further processed by a GRU layer, which estimates intermediate feature sets via equations 6.15 & 6.16 as follows,

$$z = var(W_z * [h_{out} * T_{out}]) \tag{6.15}$$

$$r = var(W_r * [h_{out} * T_{out}]) \tag{6.16}$$

Both of these, to update the kernel matrix, features are used via equation 6.17 as follows,

$$h_t' = tanh(W * [r * h_{out} * T_{out}]) \tag{6.17}$$

This kernel matrix is used to generate output features via equation 6.18,

$$xout = (1 - z) * h_t' + z * h_{out} \tag{6.18}$$

A Recurrent Neural Network (RNN) processes the output features recursively, aiding in the estimation of various disease categories. Equation 6.19 shows how the RNN model, which is represented in figure 6.3, creates disease-specific action classes by solely linear activations using supporting augmented (SA) features,

$$C_{out} = purelin(\sum_{i=1}^{N} xout_i * W_i) \tag{6.19}$$

Where, N represents total number of features extracted by different LSTM & GRU layers, while W represents respective feature weight sets.

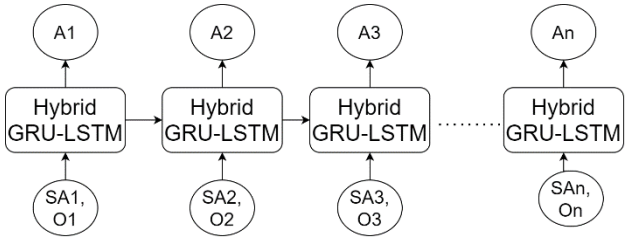


Figure 6.3 Design of the LSTM & GRU based RNN process for estimation of disease classes

Due to use of RNN, the system model is able to identify incrementally optimum features, which enhances the accuracy of classification under different disease types. Once diseases are identified, then a contextual Convolutional Neural Network (CNN) is trained & evaluated to estimate disease severity levels. Design of this CNN is depicted in figure 6.4, where a combination of different sized convolutional layers are Max Pooled cascaded together for estimation of high variance feature sets.

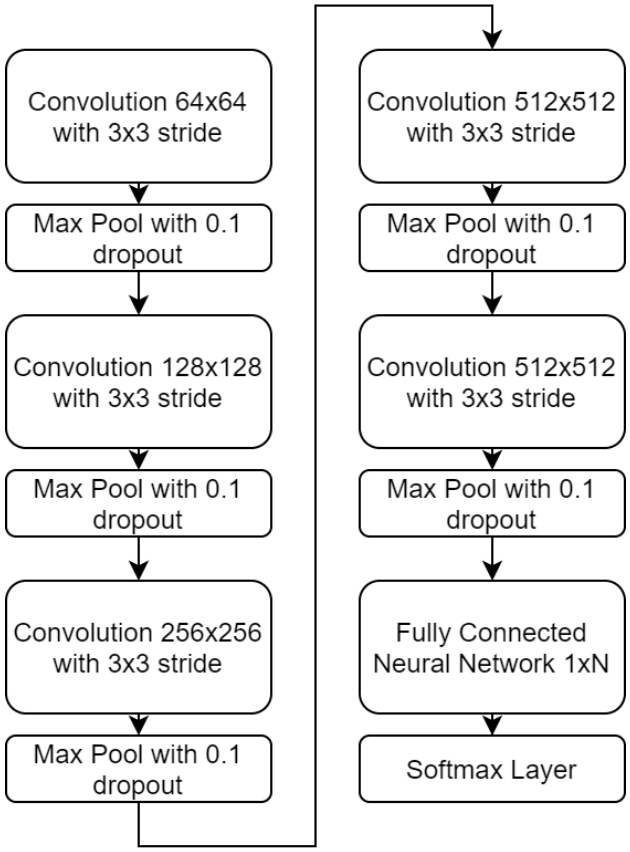


Figure 6.4. Design of the CNN Model for estimation of disease severity levels

These Max Pooling layers are further supported by Drop Out layers, that remove low variance features, thereby assisting in improving accuracy of disease severity identification for different disease types. Equation 6.20 represents the features of this model that were extracted by the convolutional layers,

$$Conv_{out_{i,j}} = \sum_{a=-\frac{m}{2}}^{\frac{m}{2}} \sum_{b=-\frac{n}{2}}^{\frac{n}{2}} I(i-a, j-b) * ReLU\left(\frac{m}{2}+a, \frac{n}{2}+b\right) \qquad (6.20)$$

Where, m, n represents the convolutional window dimensions, a, b represent stride window dimensions, while $ReLU$ represents a Rectilinear Unit, which is used for activation of these features. Due to wide variations in window sizes, a large number of convolutional features are retrieved, which adds redundancy to the feature extraction process. To reduce this redundancy, the Max Pooling layer estimates a feature variance threshold via equation 6.21,

$$f_{th} = \left(\frac{1}{X_k} * \sum_{x \in X_k} x^{p_k}\right)^{1/p_k} \qquad (6.21)$$

Where, X & p represents feature value, and its variance levels. The Max Pooling layer removes all features where the feature value $f \leq f_{th}$, thus retaining only high variance

feature sets. This process is repeated for different window sizes, and the selected features are classified using a SoftMax based activation layer, which is represented in equation 6.22,

$$c_{out} = SoftMax\left(\sum_{i=1}^{N_f} f_i * w_i + b\right) \quad (6.22)$$

Where, N_f represents number of extracted features, while w & b represents their weights & biases. The output class, which depicts various illness kinds' varying degrees of severity and can be utilised to make therapy suggestions. The suggested approach can be used for a wide range of clinical use cases because it incorporates shared blockchains with operations for disease classification and severity detection. The following section of this article discusses a comparison of the system model to existing methods in terms of various parameter sets.

6.4 Result Analysis & Comparisons

The suggested model demonstrates transparency, traceability, immutability, and distributed computing capabilities because it initially stores patient data on a single linked blockchain. However, the QoS performance of this single chained blockchain declines as the number of blocks on the chain rises, which has a negative impact on the speed and high energy consumption of the deployed medical device sets. To overcome this issue, a Proof-of-Mining Trust (PoMT) based model is deployed, which assists in selection of high trust miner nodes, thereby incrementally improving QoS levels. This PoMT Model is extended via a Genetic Chain Optimization (GCO) Model that assists in deciding optimal shard sizes for current blockchain(s). The GCO uses a combination of mining delay, residual energy of miners, their temporal throughput levels, and PDR levels in order to identify optimum shard sizes. As a result, the model may maintain high security and good quality of service for a variety of real-time application situations. The effectiveness of the model's security was assessed for the attack types of spoofing, spying, and masquerading. According to this performance evaluation, it was found that the model was 100% effective at mitigating these assaults, making it suitable for usage in real-time healthcare deployments. This QoS performance was estimated and compared to conventional blockchain-based techniques in terms of the time it took for deployed nodes to communicate with one another, the energy required for these communications, the throughput levels at each node, and the PDR levels. This performance is depicted in the text's subsequent subsection.

6.4.1. Performance in terms of QoS parameters under different attack types

As discussed earlier, the model was able to mitigate multiple attack types with high efficiency, while maintaining high QoS levels w.r.t. existing methods. These QoS levels were evaluated for a hospital with different number of sensors. These sensors were varied between 500 to 2000 and included Temperature, Humidity, Blood Pressure, Heart Rate, Electrocardiogram (ECG), etc. While performing sensor-to-base station communications, the average communication delay (D) for these requests was estimated for different communication requests (CR), and compared with FB [4], NTM [15], and IPHL [25] in table 6.2, where 10% of all communication requests were stochastically passed as attack packets.

Table 6.2. Delay during different device communications under multiple attacks

No. of Sensors 500, 1000, 2000				
CR	**D (ms) FB [4]**	**D (ms) NTM [15]**	**D (ms) IPHL [25]**	**D (ms) BDSIHD**
1250	1.23	1.35	1.21	1.07
1500	1.30	1.43	1.28	1.13
1750	1.37	1.51	1.35	1.21
2000	1.45	1.63	1.47	1.35
2250	1.61	1.86	1.71	1.59
2500	1.93	2.26	2.08	1.93
3125	2.38	2.77	2.53	2.32
3750	2.88	3.28	2.97	2.68
5000	3.30	3.72	3.35	3.02
5625	3.69	4.15	3.74	3.38
6250	4.11	4.63	4.19	3.76
6875	4.62	5.21	4.68	4.14
7500	5.04	5.72	5.12	4.44
8750	5.38	6.12	5.45	4.67
10000	5.57	6.36	5.67	4.87
12500	5.81	6.63	5.92	5.50

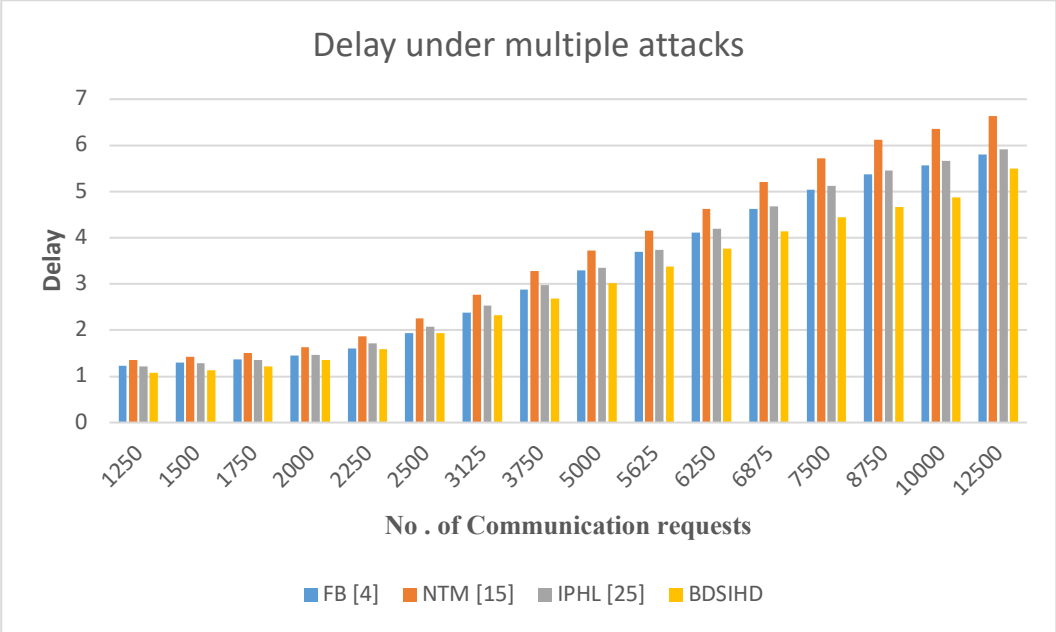


Figure 6.5. Delay during different device communications under multiple attacks

The evaluation and figure 6.5 show that the proposed model outperformed the competition in terms of communication speed, outperforming FB [4], NTM [15], and IPHL [25] by 3.5%, 10.4%, and 8.5%, respectively. This makes the model extremely valuable for a range of real-time clinical deployments. This improvement is due to the PoMT model's usage of distance measurements, which helps choose low-delay nodes for various deployment scenarios. As a result, the model can be used to many different high-speed deployment scenarios. In a similar vein, table 6.3 displays the energy use as follows:

Table 6.3. Energy needed during different device communications under multiple attacks

No. of Sensors				**500, 1000, 2000**
CR	**E (mJ) FB [4]**	**E (mJ) NTM [15]**	**E (mJ) IPHL [25]**	**E (mJ) BDSIHD**
1250	3.57	4.06	3.31	3.08
1500	3.84	4.33	3.53	3.27
1750	4.05	4.58	3.72	3.45
2000	4.28	4.82	3.91	3.62
2250	4.49	5.04	4.09	3.78
2500	4.68	5.25	4.26	3.94
3125	4.87	5.48	4.45	4.14
3750	5.11	5.77	4.70	4.37
5000	5.41	6.11	4.96	4.62
5625	5.74	6.44	5.21	4.85
6250	6.04	6.71	5.41	5.04
6875	6.28	6.95	5.60	5.22
7500	6.50	7.19	5.79	5.40

8750	6.73	7.45	6.00	5.60
10000	6.96	7.71	6.21	5.79
12500	7.20	7.97	6.42	5.98

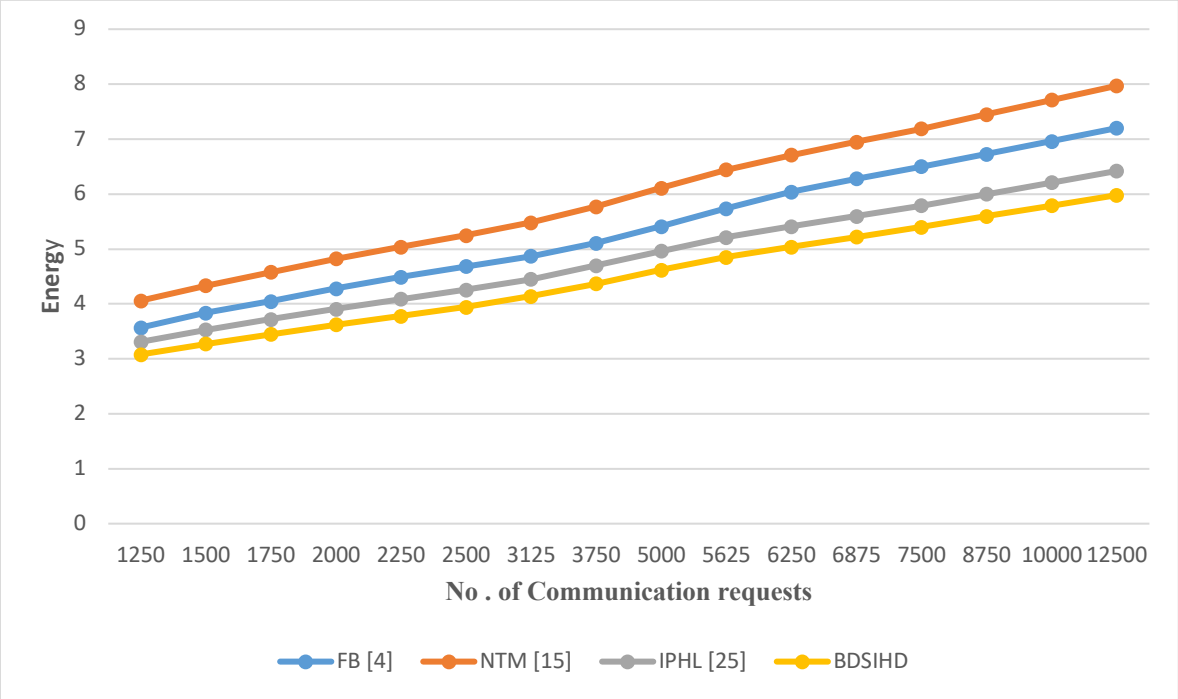


Figure 6.6. Energy needed during different device communications under multiple attacks

According to this assessment and figure 6.6, the suggested model was shown to be highly beneficial for high-lifetime clinical use cases since it was able to cut energy usage by 10.5% when compared with FB [4], 14.6% when compared with NTM [15], and 5.9% when compared with IPHL [25]. This improvement results from the PoMT model's utilization of residual node energy, which helps choose high energy nodes for various deployment circumstances. As a result, the model can be used to many different high-lifetime deployment scenarios. Similarly, table 6.4 shows the throughput during these communications as follows,

Table 6.4. Throughput performance during different device communications under multiple attacks

No. Of Sensors				**500, 1000, 2000**
CR	**T (kbps) FB [4]**	**T (kbps) NTM [15]**	**T (kbps) IPHL [25]**	**T (kbps) BDSIHD**
1250	355.25	391.14	421.26	532.98
1500	358.12	394.31	424.70	537.41
1750	361.07	397.64	428.32	542.00
2000	364.22	401.10	432.04	546.66
2250	367.36	404.54	435.73	551.27
2500	370.42	407.91	439.36	555.83

3125	373.48	411.28	442.99	560.40
3750	376.54	414.64	446.60	564.97
5000	379.61	418.00	450.22	569.54
5625	382.69	421.37	453.83	574.12
6250	385.78	424.76	457.45	578.70
6875	388.85	428.12	461.05	583.24
7500	391.90	431.45	464.64	587.78
8750	394.93	434.77	468.21	592.30
10000	397.97	438.11	471.83	596.85
12500	401.03	441.48	475.45	601.41

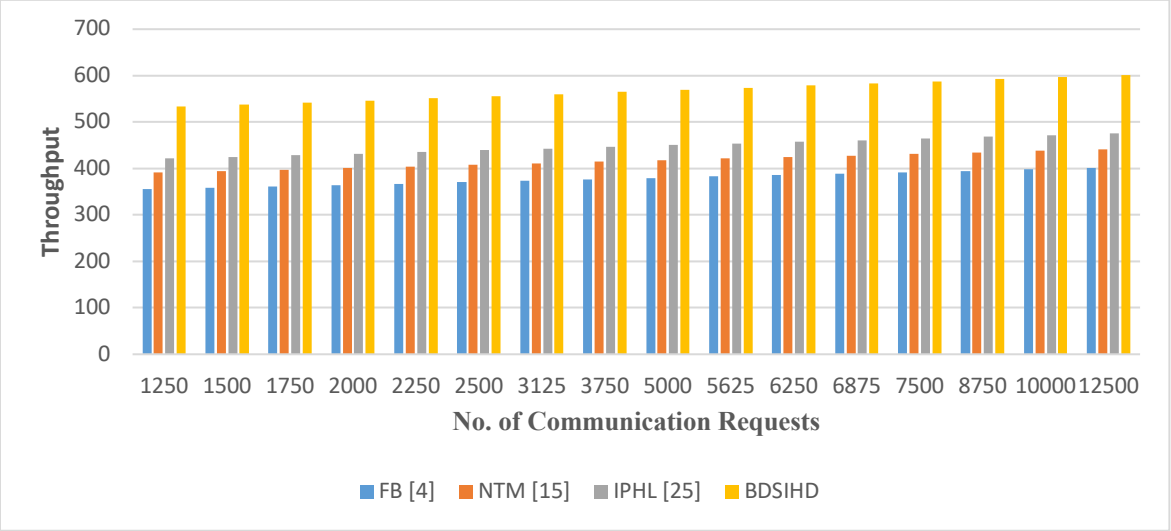


Figure 6.7. Throughput performance during different device communications under multiple attacks

According to this assessment and figure 6.7, the suggested model outperformed FB [4], NTM [15], and IPHL [25] in terms of throughput performance, improving it by 23.9%, 19.4%, and 15.5%, respectively. This indicates that the model is very beneficial for high-data-rate installations. This improvement is due to the PoMT model's utilization of temporal throughput levels, which help choose high-performance nodes for various deployment scenarios. Because of this, the approach can be applied to many different high-throughput deployment scenarios. Similarly, table 6.5 shows the PDR during these communications as follows.

Table 6.5. Packet Delivery Ratio performance during different device communications under multiple attacks

No. Of Sensors				500, 1000, 2000
CR	PDR (%) FB [4]	PDR (%) NTM [15]	PDR (%) IPHL [25]	PDR (%) BDSIHD
1250	79.19	79.45	82.75	81.43
1500	79.83	80.10	83.42	82.10
1750	80.49	80.77	84.13	82.80
2000	81.19	81.47	84.86	83.52
2250	81.89	82.17	85.58	84.22
2500	82.58	82.85	86.29	84.92
3125	83.26	83.53	87.00	85.62
3750	83.95	84.22	87.71	86.32
5000	84.63	84.90	88.43	87.02
5625	85.31	85.59	89.14	87.71
6250	86.00	86.27	89.85	88.41
6875	86.68	86.95	90.56	89.11
7500	87.36	87.64	91.27	89.81
8750	88.05	88.32	91.98	90.51
10000	88.73	89.00	92.68	94.69
12500	89.41	89.68	93.39	98.90

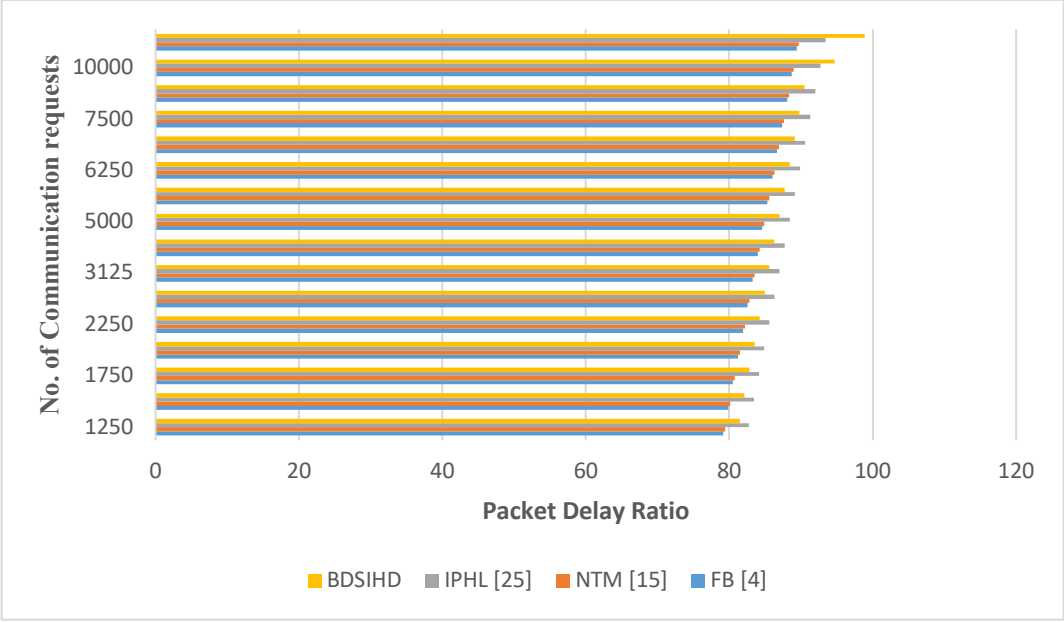


Figure 6.8. PDR performance during different device communications under multiple attacks

According to this evaluation and figure 6.8, the suggested model was found to be very helpful for high-consistency deployments since it was able to increase PDR performance by 9.5% when compared with FB [4], 8.3% when compared with NTM [15], and 6.5% when compared with IPHL [25]. This improvement results from the PoMT model's

utilization of temporal PDR levels, which helps choose high-performance nodes for various deployment scenarios. Because of this, the model may be applied to many different high-consistency and low-data-drop deployment scenarios. The proposed model can be implemented for many real-time clinical scenarios as a result of these improvements. The categorization performance for various illness kinds was also assessed in a manner similar to this one, and it was covered in the next section of this.

6.4.2 Classification performance of the proposed model for different disease types

Once the model is deployed for clinical scenarios, its classification performance must be evaluated so that the model is able to assist doctors in identification of different disease types, and their severity levels. This performance was estimated in terms of accuracy (A), precision (P), and recall (R), levels on the following data sets,

- WUSTL EHMS 2020 Dataset, that is available at https://www.cse.wustl.edu/~jain/ehms/index.html
- BPCO dataset, which is available at https://www.kaggle.com/datasets/cnrieiit/bpco-dataset-based-gans-for-iomt
- MIMIC-III dataset, which is available at https://www.kaggle.com/datasets/asjad99/mimiciii

After combining all of these sets, a total of 18000 records were created, comprising 4 severity levels and 5 illness categories. Of these records, 1500 were used for testing and validation procedures, and 15000 were used for training. With respect to varying numbers of test samples (NTS) in table 6.6, the accuracy of classification based on this technique was assessed using equation 6.23 and compared with FB [4], NTM [15], and IPHL [25],

$$A_R = \frac{D_C}{D_T} \tag{6.23}$$

Where, $D_C \; and \; D_T$ represents number of correctly classified disease types, and total number of disease types.

Table 6.6. Accuracy levels for classification of different diseases

NTS	A_R DL [26]	A_R ABM CGC LSTM [40]	A_R RCNN [101]	A_R BDSIHD
540	80.51	77.05	80.77	86.16
1080	81.54	78.31	81.82	87.25
1620	82.56	79.56	82.85	88.48
2160	83.85	80.95	84.13	89.84
2700	85.13	82.33	85.41	91.07
3240	86.15	83.59	86.44	91.42
3780	85.77	83.03	86.05	90.98
4320	85.33	82.13	85.62	91.09
4860	85.97	82.82	86.28	91.61
5400	86.31	83.31	86.62	91.78
6300	86.31	83.59	86.62	91.81
7200	86.36	83.85	86.67	92.01
8100	86.69	84.15	86.97	92.29
9000	86.87	84.26	87.15	92.52
9900	87.13	84.49	87.44	92.85
10800	87.49	84.90	87.79	93.17
11700	87.74	85.21	88.05	93.45
12600	88.00	85.49	88.28	93.71
13500	88.23	85.74	88.51	93.92
14400	88.41	85.97	88.72	94.13
15300	88.62	86.23	88.92	94.36
16200	88.85	86.51	89.13	94.62
17100	89.10	86.79	89.36	94.88
18000	89.35	87.06	89.59	95.14

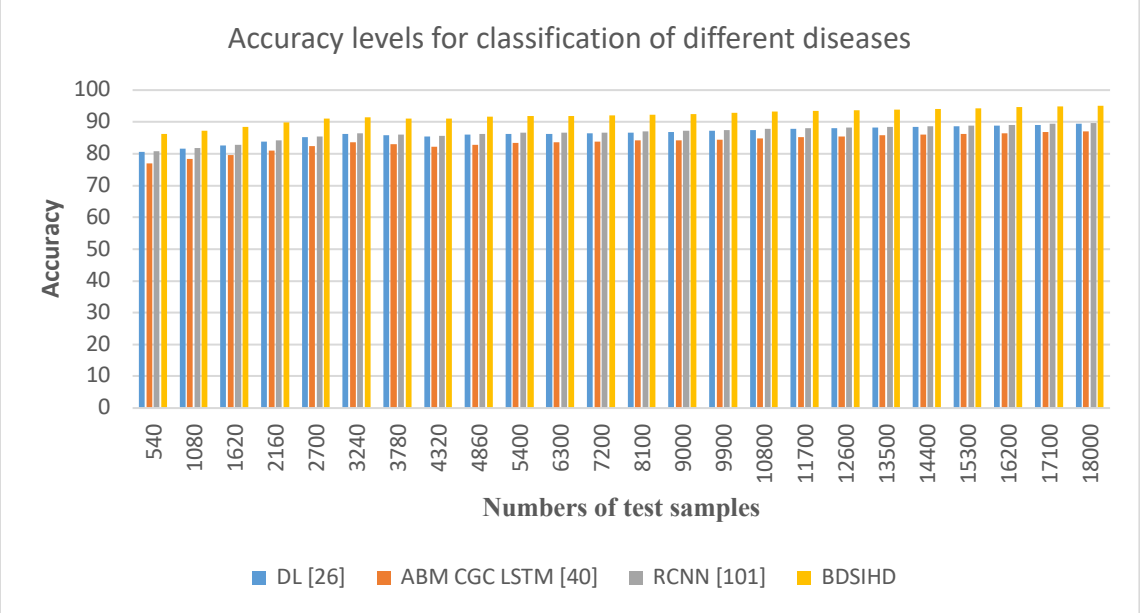


Figure 6.9. Accuracy levels for classification of different diseases

According to this analysis and figure 6.9, the suggested model demonstrated 5.4% higher classification accuracy than DL [26], 8.3% higher accuracy than ABM CGC LSTM [40], and 4.9% higher accuracy than RCNN [101]. This indicates that the model is very beneficial for a wide range of real-time clinical use cases. The combination of LSTM & GRU with RNN for feature set categorization representation improves accuracy. In a similar manner, table 6.7's precision levels were calculated and tallied as follows,

Table 6.7. Precision levels for classification of different diseases

NTS	P_R **DL [26]**	P_R **ABM CGC LSTM [40]**	P_R **RCNN [101]**	P_R **BDSIHD**
540	77.67	75.90	78.72	83.10
1080	78.64	77.13	79.72	84.15
1620	79.64	78.36	80.72	85.35
2160	80.90	79.74	81.97	86.69
2700	82.15	81.10	83.21	87.89
3240	83.15	82.33	84.21	88.22
3780	82.77	81.77	83.85	87.77
4320	82.31	80.87	83.44	87.85
4860	82.92	81.56	84.05	88.37
5400	83.28	82.08	84.36	88.58
6300	83.31	82.36	84.38	88.60
7200	83.33	82.59	84.44	88.77
8100	83.62	82.87	84.74	89.01
9000	83.79	82.97	84.92	89.24
9900	84.05	83.21	85.18	89.57
10800	84.41	83.62	85.54	89.90
11700	84.67	83.92	85.79	90.14
12600	84.87	84.18	86.03	90.37
13500	85.10	84.44	86.26	90.61
14400	85.31	84.69	86.46	90.81
15300	85.49	84.95	86.67	91.03
16200	85.72	85.23	86.87	91.29
17100	85.97	85.51	87.10	91.73
18000	86.55	86.13	87.70	92.35

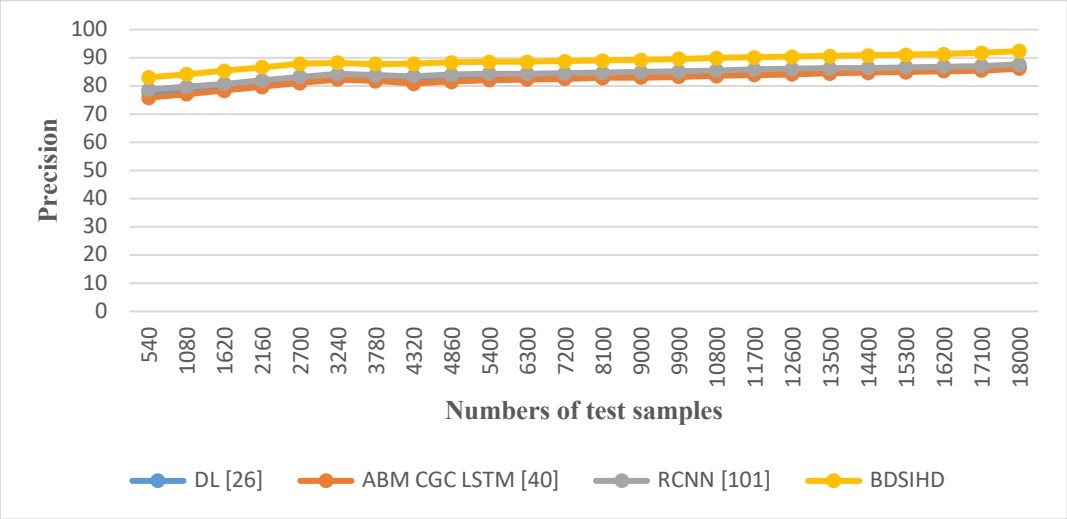


Figure 6.10. Precision levels for classification of different diseases

As per this analysis, and figure 6.10, it can be observed that the proposed model showcased 5.9% higher precision of classification than DL [26], 5.4% higher precision than ABM CGC LSTM [40], and 4.6% higher precision than RCNN [101], which makes it highly useful for consistency-aware real-time clinical use cases. This precision is improved due to combination of LSTM & GRU that enable extraction of consistent feature sets, and RNN for classification of these feature sets. Similarly, the recall levels were estimated and tabulated in table 6.8 as follows

Table 6.8 Recall levels for classification of different diseases

NTS	R_R DL [26]	R_R ABM CGC LSTM [40]	R_R RCNN [101]	R_R BDSIHD
540	67.46	66.64	71.41	72.30
1080	68.36	67.74	72.31	73.24
1620	69.23	68.85	73.23	74.27
2160	70.31	70.03	74.36	75.44
2700	71.41	71.21	75.49	76.50
3240	72.31	72.31	76.41	76.79
3780	71.95	71.79	76.05	76.37
4320	71.51	70.97	75.64	76.44
4860	72.08	71.59	76.23	76.91
5400	72.41	72.08	76.56	77.11
6300	72.44	72.36	76.59	77.13
7200	72.46	72.54	76.59	77.30
8100	72.74	72.77	76.85	77.54
9000	72.92	72.90	77.03	77.75
9900	73.13	73.10	77.26	78.01
10800	73.41	73.44	77.59	78.28
11700	73.64	73.72	77.85	78.51
12600	73.85	73.95	78.03	78.73

13500	74.05	74.18	78.23	78.95
14400	74.26	74.44	78.44	79.14
15300	74.41	74.64	78.59	79.30
16200	74.56	74.85	78.77	79.51
17100	74.79	75.10	79.00	79.91
18000	75.32	75.67	79.54	80.47

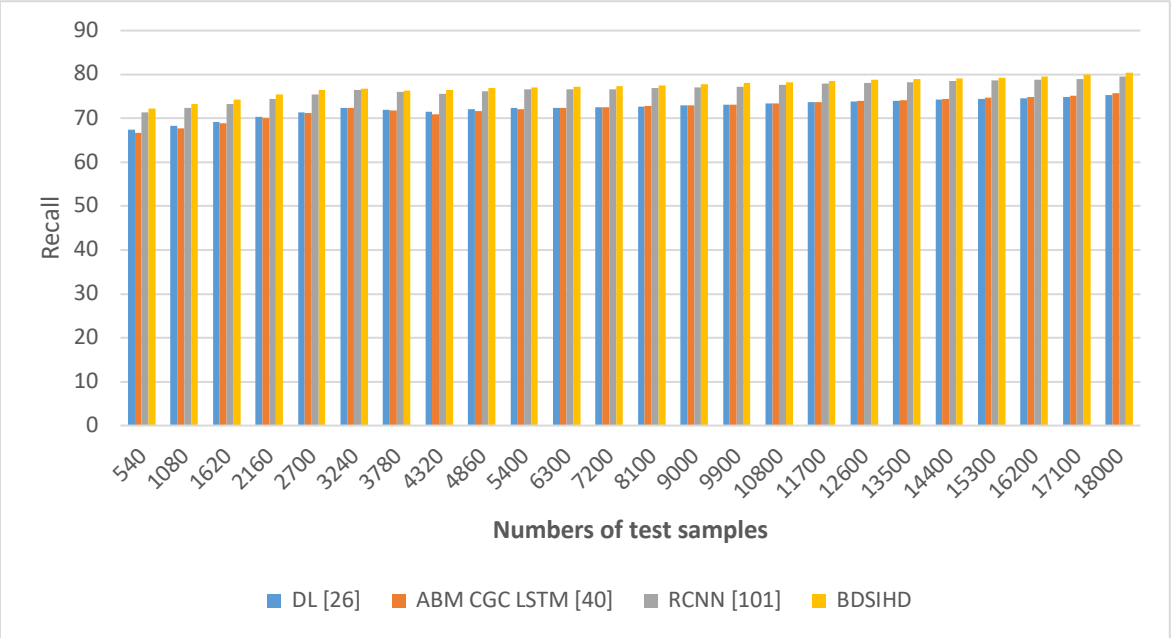


Figure 6.11. Recall levels for classification of different diseases

As per this analysis, and figure 6.11, it can be observed that the proposed model showcased 4.5% higher recall of classification than DL [26], 4.1% higher recall than ABM CGC LSTM [40], and 1.9% higher recall than RCNN [101], which makes it highly useful for consistency-aware clinical use cases. This recall is improved due to combination of LSTM & GRU that enable extraction of consistent feature sets, and RNN for classification of these feature sets. Similarly, the accuracy levels for severity detection were estimated and tabulated in table 6.9 as follows,

Table 6.9. Accuracy of severity level estimation for classification of different diseases

NTS	**AS_R DL [26]**	**AS_R ABM CGC LSTM [40]**	**AS_R RCNN [101]**	**AS_R BDSIHD**
540	72.13	70.92	74.74	77.23
1080	73.05	72.10	75.72	78.23
1620	74.00	73.26	76.67	79.36
2160	75.18	74.51	77.85	80.60
2700	76.33	75.79	79.05	81.71
3240	77.26	76.95	80.00	82.02

3780	76.90	76.41	79.64	81.61
4320	76.49	75.59	79.26	81.71
4860	77.10	76.26	79.85	82.20
5400	77.41	76.72	80.15	82.38
6300	77.44	76.97	80.18	82.42
7200	77.49	77.18	80.21	82.59
8100	77.74	77.44	80.49	82.82
9000	77.92	77.59	80.69	83.04
9900	78.15	77.82	80.95	83.32
10800	78.46	78.15	81.26	83.62
11700	78.72	78.44	81.49	83.87
12600	78.92	78.69	81.69	84.10
13500	79.15	78.95	81.92	84.32
14400	79.33	79.18	82.13	84.50
15300	79.49	79.38	82.28	84.70
16200	79.72	79.64	82.46	84.94
17100	79.95	79.95	82.72	85.35
18000	80.48	80.54	83.30	85.94

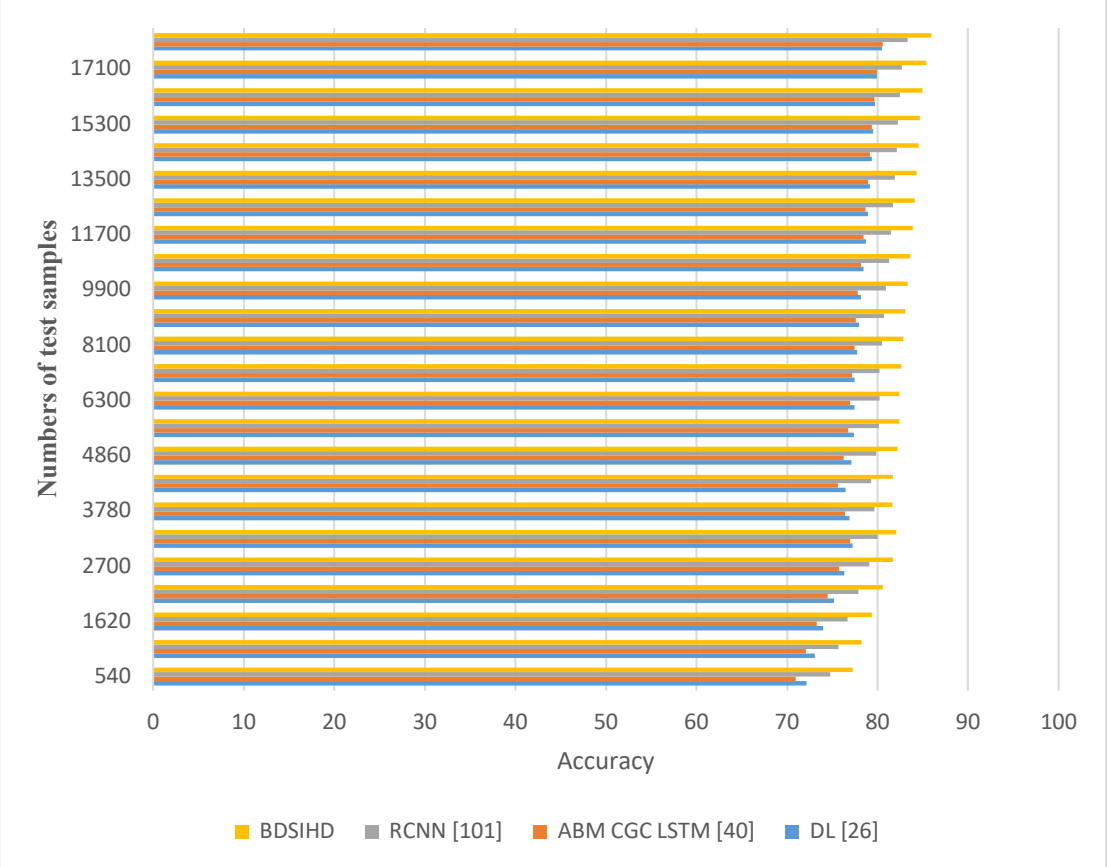


Figure 6.12. Accuracy of severity level estimation for classification of different diseases

As per this analysis, and figure 6.12, it can be observed that the proposed model showcased 5.5% higher accuracy of severity detection than DL [26], 5.4% higher accuracy of severity detection than ABM CGC LSTM [40], and 2.9% higher severity than RCNN [101], which makes it highly useful for alerting applications, where doctors are needed to be alerted as per patient's disease progressions. This accuracy is improved due to use of customized CNN, which assists in efficient for identification of severity levels from classified sets. These improvements enable the suggested approach to be implemented for high-speed, highly secure, and high quality of service clinical applications.

6.5 Conclusion

The system model exhibits transparency, traceability, immutability, and distributed computing capabilities because it initially stores patient data on a single chained blockchain. However, the QoS performance of this single chained blockchain declines as the number of blocks on the chain rises, which has a negative impact on the speed and high energy consumption of the deployed medical device sets. A Proof-of-Mining Trust (PoMT) based model is implemented to address this problem and aid in the selection of high trust miner nodes, thereby gradually raising QoS levels. The PoMT Model (s) is extended by a Genetic Chain Optimisation (GCO) Model that assists in selecting the optimal shard sizes for the current blockchain. The GCO combines mining delay, miners' residual energy, their temporal throughput levels, and PDR levels to estimate the optimal shard sizes. The model may therefore maintain high security and good QoS for a variety of real-time use scenarios. The effectiveness of the model's security was assessed for the attack types of spoofing, snooping, and masquerade. The model was 100% successful in mitigating these assaults, according to this performance evaluation, making it appropriate for usage in real-time healthcare installations. The system model was shown to be particularly helpful for a range of real-time clinical deployments because it was able to boost communication speed by 3.5% when compared to FB [4], 10.4% when compared to NTM [15], and 8.5% when compared to IPHL [25]. The PoMT model's use of distance measurements, which aids in the selection of low-delay nodes for various deployment circumstances, is responsible for this improvement. As a result, the concept can be used for numerous alternative high-speed deployments.

It was discovered that the system model is very beneficial for high-lifetime clinical use cases since it may cut energy consumption by 10.5% when compared to FB [4], 14.6%

when compared to NTM [15], and 5.9% when compared to IPHL [25]. This improvement is due to the PoMT model's use of residual node energy, which helps in the selection of high-energy nodes for various deployment scenarios. The model can be applied to many different high-lifetime deployments as a result. The system model was found to be very helpful for high-data-rate deployments, increasing throughput performance in terms of communication data rate by 23.9% when compared to FB [4], 19.4% when compared to NTM [15], and 15.5% when compared to IPHL [25]. This improvement is due to the PoMT model's use of temporal throughput levels, which helps in the selection of high-performance nodes for various deployment scenarios. As a result, the model can be used in numerous high-throughput installations. While it was discovered that the system model was able to significantly improve PDR performance in terms of packet consistency when compared to FB [4], NTM [15], and IPHL [25], increasing it by 9.5%, 8.3%, and 6.5% respectively, making it incredibly useful for high-consistency deployments. This improvement is due to the PoMT model's use of temporal PDR levels, which aid in the selection of high-performance nodes for various deployment scenarios. The model can be applied to a wide range of high-consistency & low-data-drop deployments as a result. These upgrades make it possible to use the suggested model in a variety of real-time clinical circumstances.

It is necessary to evaluate the model's classification performance once it has been applied to clinical scenarios so that it can aid medical professionals in identifying distinct illness kinds and the severity of each one. The suggested model showed classification accuracy that was 5.4% more than that of DL [26], 8.3% greater than that of ABM CGC LSTM [40], and 4.9% greater than that of RCNN [101] according to accuracy analysis, making it very beneficial for a range of real-time clinical use cases. The combination of LSTM and GRU with RNN for feature set classification representation improves accuracy. According to consistency analysis, the system model demonstrated classification precision that was 5.9% higher than DL [26], 5.4% higher than ABM CGC LSTM [40], and 4.6% higher than RCNN [101], making it extremely useful for consistency-aware real-time clinical use cases. The combination of LSTM and GRU, which enables the extraction of consistent feature sets, and RNN, which allows the classification of these feature sets, improves this precision. According to recall evaluations, the proposed model demonstrated recall of classification that was 4.5% higher than DL [26], 4.1% higher than ABM CGC LSTM [40], and 1.9% higher than RCNN [101], making it extremely useful for consistency-aware clinical use cases. Recall is increased by combining LSTM and

GRU, which allow for the extraction of consistent feature sets, with RNN, which categorises these feature sets. The system model displayed 5.5% higher accuracy of severity identification than DL [26], 5.4% higher accuracy of severity detection than ABM CGC LSTM [40], and 2.9% higher severity than RCNN [101] in terms of severity analysis. It is therefore very helpful for alerting applications, where doctors need to be informed as patients' illnesses worsen. This accuracy is enhanced by the application of a tailored CNN, which facilitates the recognition of severity levels from categorised sets. As a result, it is extremely useful for alerting applications, where doctors need to be alerted as patients' diseases advance. The use of a customized CNN, which makes it easier to identify severity levels from categorized sets, improves this accuracy. These improvements enable the system model to be deployed for clinical scenarios requiring high QoS, high speed, and high security levels.

Future performance testing of this model under real-world conditions is necessary, and it can be improved by utilising Q-Learning, Transformer Networks, Auto Encoder Networks, and Generative Adversarial Networks (GANs). This performance can also be improved by combining several bioinspired models, which will help to gradually raise the levels of disease classification and severity estimation in real-world scenarios.

CHAPTER 7

Results and Discussions

Table 7.1 Recovery duration for patients with high blood sugar levels for 200 patients in days

Expected Average recovery by using [11]	Expected Average recovery by using [15]	Expected Average recovery by using proposed model
3.8	2.9	1.3

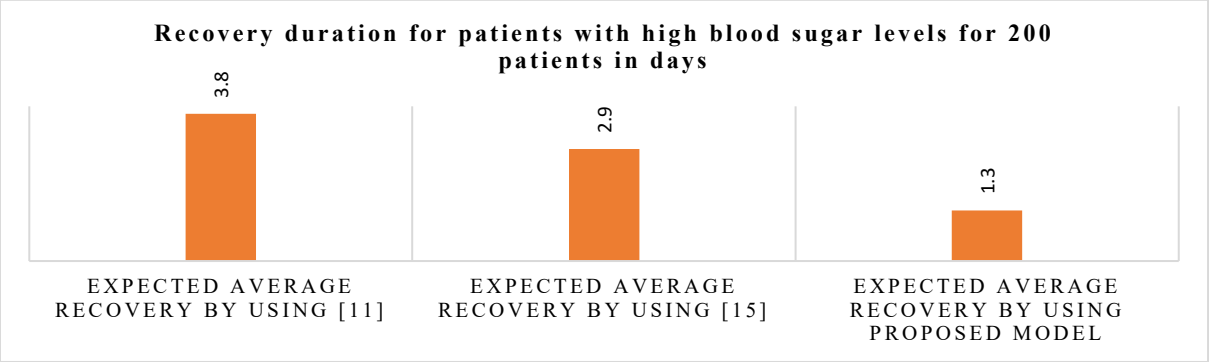


Figure 7.1 : Recovery duration for patients with high blood sugar levels for 200 patients in days

Table 7.2 : Recovery duration for patients with lung cancer condition of 200 patients in fortnights

Expected Average recovery by using [11]	Expected Average recovery by using [15]	Expected Average recovery by using proposed model in Months
3.8	2.9	1.3

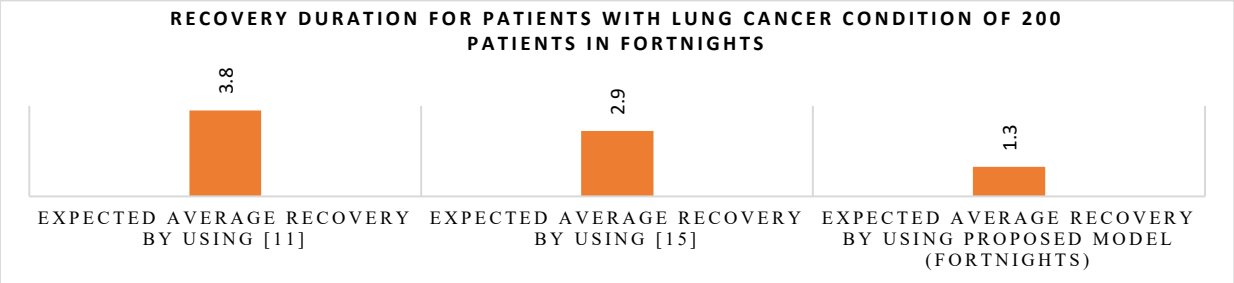


Figure7.2 Recovery duration for patients with lung cancer condition of 200 patients in fortnights

Table 7.3: Recovery duration for patients with lung cancer condition of 200 patients in fortnights

Expected Average recovery by using [11]	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model (fortnights)**
3.8	2.9	1.3

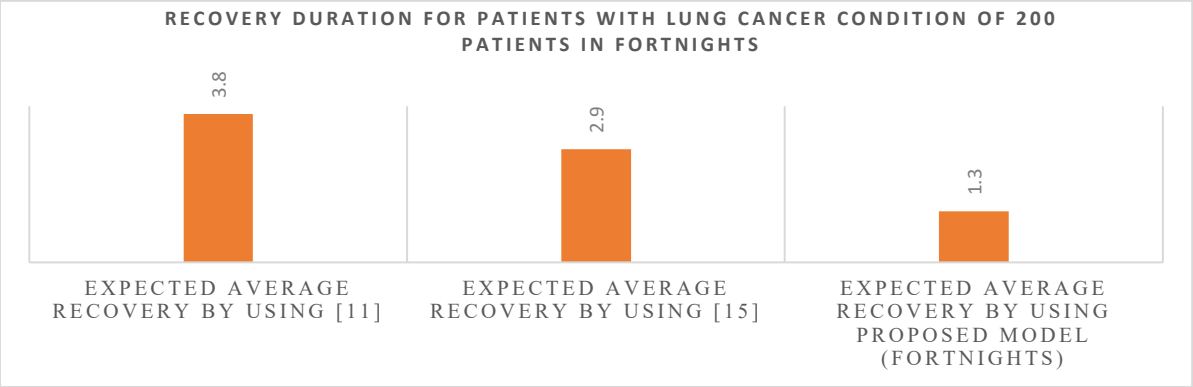


Figure 7.3: Recovery duration for patients with lung cancer condition of 200 patients in fortnights

Table 7.4 : Recovery duration for patients with diabetic retinopathy conditioning in weeks

Expected Average recovery by using [11]	**Expected Average recovery by using [15]**	**Expected Average recovery by using proposed model in weeks**
3.8	2.9	1.3

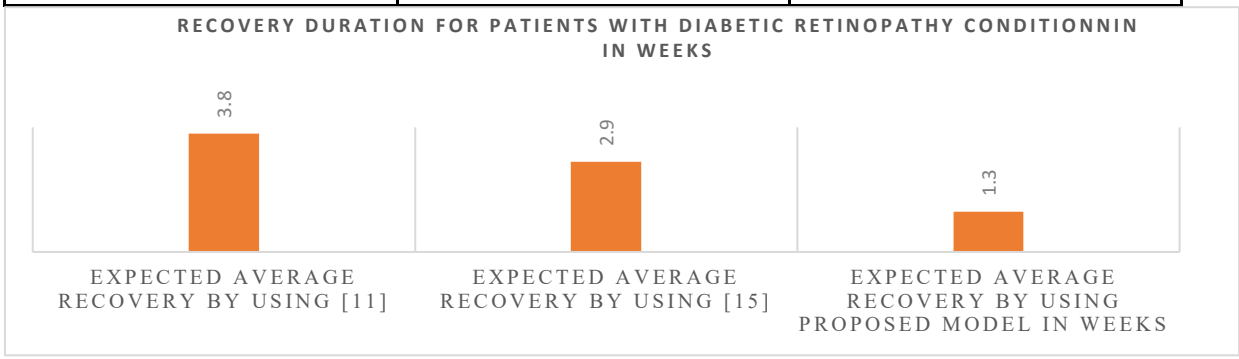


Figure 7.4 Recovery duration for patients with diabetic retinopathy conditioning in weeks

Table 7.5 Average end-to-end delay for various blockchain communication

No. of Patients 5000			
D (ms) LSR DM EH [35]	**D (ms) LCDL [42]**	**D (ms) BEC [48]**	**D (ms) Proposed**
4.22	5.09	5.56	3.89

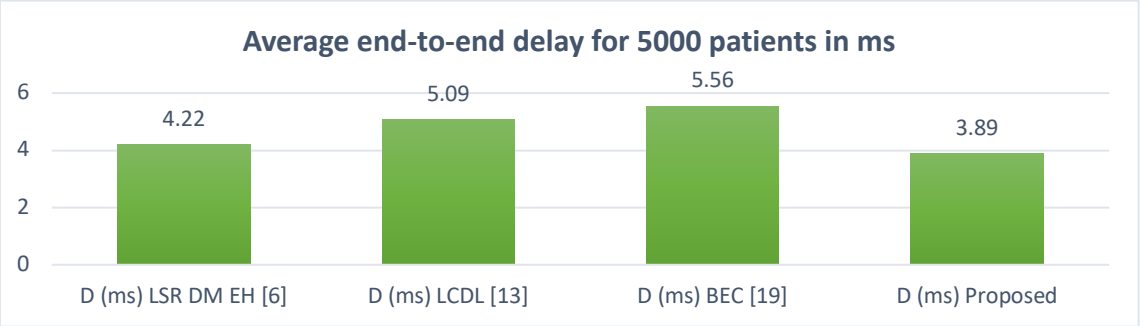


Figure 7.5 Average end-to-end delay for various blockchain communication

Table 7.6 Average end-to-end Energy for 5000 patients in mJ

E (mJ) LSR DM EH [35]	**E (mJ) LCDL [42]**	**E (mJ) BEC [48]**	**E (mJ) Proposed**
4.275	6.183	5.382	3.933

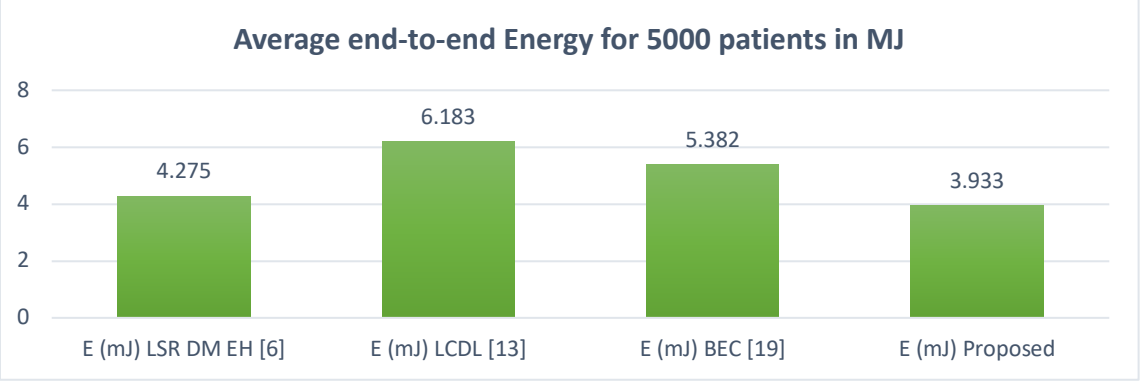


Figure 7.6 Average end-to-end Energy for 5000 patients in mJ

Table 7.7 Average throughput for 5000 patients in Kbps

T (kbps) LSR DM EH [35]	T (kbps) LCDL [42]	T (kbps) BEC [48]	T (kbps) Proposed
292.248	304.704	352.413	355.266

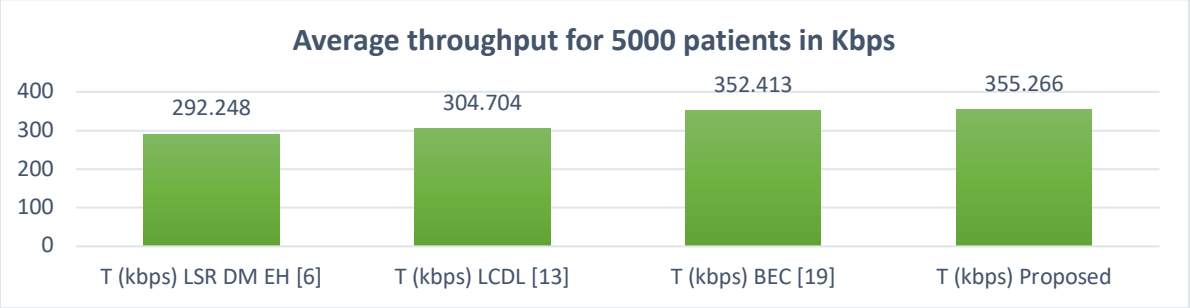


Figure 7.7 Average throughput for 5000 patients in Kbps

Table 7.8 Average packet delivery ratio for 5000 patients

PDR (%) LSR DM EH [35]	PDR (%) LCDL [42]	PDR (%) BEC [48]	PDR (%) Proposed
82.728	82.305	83.223	89.163

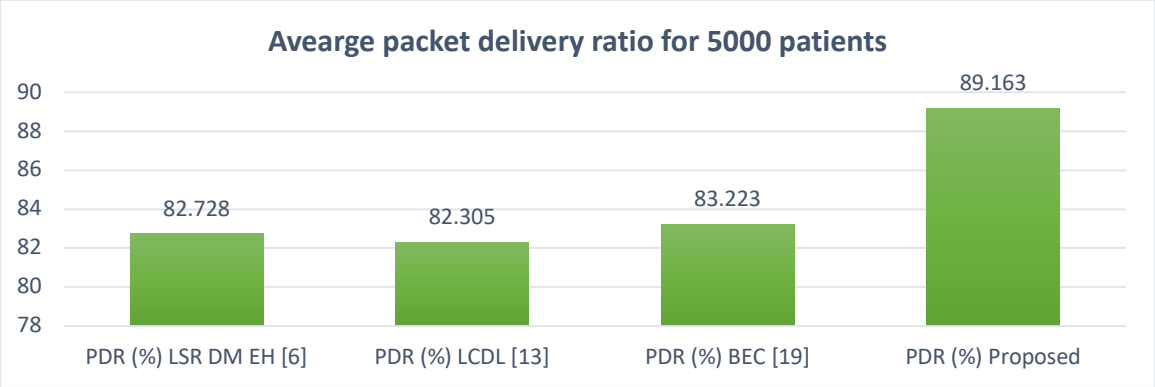


Figure 7.8 Average packet delivery ratio for 5000 patient

Table 7.9 Average delay for various attacks for 25 number of attacker

Number of attackers 25			
D (ms) LSR DM EH [35]	**D (ms) LCDL [42]**	**D (ms) BEC [48]**	**D (ms) Proposed**
4.302	4.788	4.653	3.708

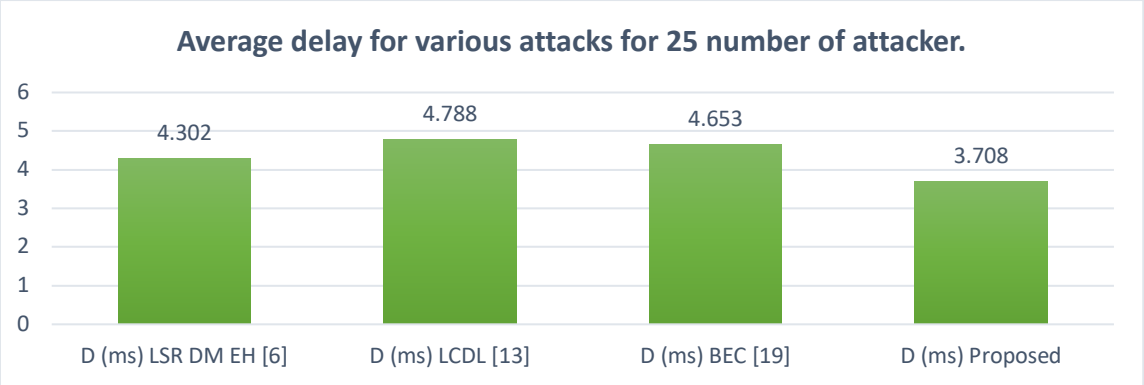


Figure 7.9 Average delay for various attacks for 25 number of attacker

Table 7.10 Average energy consumption for different attacks for 25 number of attacker

Number of attackers 25			
E (mJ) LSR DM EH [35]	**E (mJ) LCDL [42]**	**E (mJ) BEC [48]**	**E (mJ) Proposed**
5.679	5.895	5.454	4.185

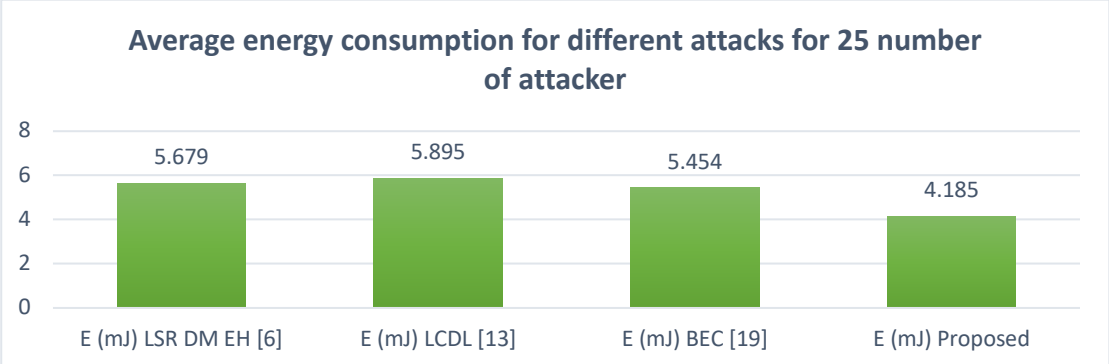


Figure 7.10 Average energy consumption for different attacks for 25 number of attacker

Table 7.11 Average throughput performance for various attacks for 25 No. of attackers

LSR DM EH [35]T (kbps)	LCDL [42]T (kbps)	BEC [48]T (kbps)	ProposedT (kbps)
317.718	338.292	322.443	439.722

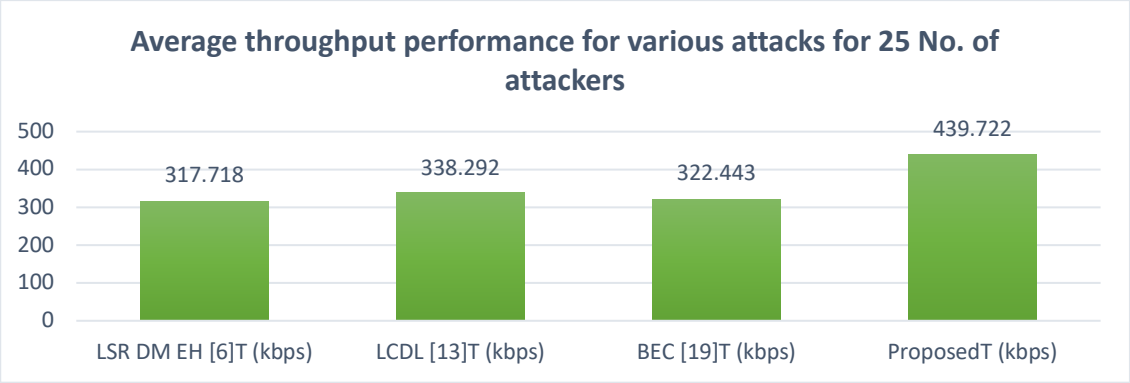


Figure 7.11 Average throughput performance for various attacks for 25 No. of attackers

Table 7.12 Average packet delivery ratio performance No. of 25 attackers

LSR DM EH [35] PDR (%)	LCDL [42] PDR (%)	BEC [48] PDR (%)	Proposed PDR (%)
62.883	60.237	66.132	89.955

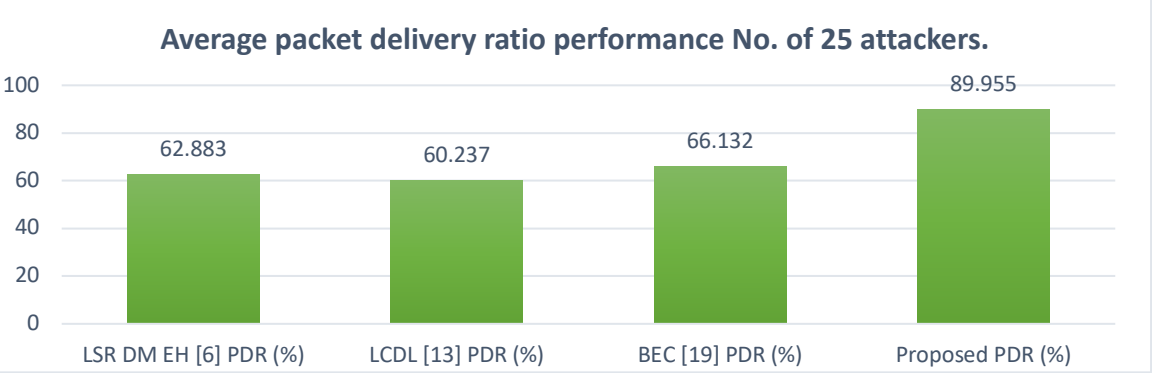


Figure 7.12 Average packet delivery ratio performance No. of 25 attackers

CHAPTER 8

Conclusion and Future Work

This chapter provides the findings from the proposed research work, advantages, disadvantages and challenges in the research work carried out. It provides the future direction for the improvement in the current research work for possible improvement.

8.1 Conclusion

This paper mentions Covid, heart disease, and diabetes models to help system designers analyze and create healthcare IoT systems for enhanced overall system performance. These models are evaluated on many patient datasets. The technology outperformed previous methods and improved patient health 15% quicker. The system is tested against 4 illnesses, and for every ailment, the suggested model speeds up patient progress. The model may be enhanced by testing it on more patients and considering other disorders when analyzing system performance. Complicated deep learning models may be employed to assess the system as the number of illnesses rises.

The suggested paradigm incorporates security and QoS by fusing GA and IQL. This enhances the model's performance under network risks in terms of latency, energy consumption, throughput, and PDR. The model combines the IQL Method, which dynamically grows blockchains, and the GA Model, which predicts sidechain configurations. The IQL Method builds incentive functions utilising a block batch assessment of the temporal quality of service. Chain expansion, aggregation, and splitting tactics are assessed, and the incremental values of these functions are looked at. Comparing the system model to LSR DM EH [35], LCDL [42], and BEC [48], it has a shorter latency. It utilises less energy than LSR DM EH [35], LCDL [42], and BEC [48] because to energy-conscious mining and sidechain selection. The model's throughput is 25.5% higher than LSR DM EH [35], LCDL [42], and BEC [48], yet similar to them. The model's PDR is higher when compared to LSR DM EH [35], LCDL [42], and BEC [48]. It uses PDR for mining and choosing sidechains. The suggested model performs better overall across deployment scenarios as a result, and its quality-of-service levels go up. The suggested model performs 15.5%, 18.3%, and 16.5% better than LSR DM EH [35], LCDL [42], and BEC [8], respectively. The system model uses 16.5%, 18.5%, and 18.3% less energy than LSR DM EH [35], LCDL [42], and BEC [48], respectively. By delivering enhanced QoS despite a range of attack types, this improvement in energy consumption performance shows that the suggested model is immune to network attacks. The idea can

be applied to real-time healthcare installations under a variety of threat scenarios. (Example) Future study will increase the model's performance utilizing deep learning techniques like CNNs, RNNs, and others. These models must be evaluated on real-time datasets to determine their scalability under various scenarios. Researchers may cascade bioinspired models to increase sidechaining performance for deployment-specific use cases.

The suggested solution holds patient data on a single linked blockchain for transparency, traceability, immutability, and distributed computing. The QoS performance of this single chained blockchain declines as the number of blocks on the chain rises, impacting the speed and energy use of deployed medical device sets. PoMT is developed to overcome this issue and pick high-trust miner nodes, progressively boosting QoS levels. The PoMT Model is extended with a GCO Model to identify the appropriate blockchain shard sizes (s). GCO uses mining latency, miners' leftover energy, temporal throughput, and PDR to estimate shard sizes. This ensures strong security and QoS for real-time use cases. Spoofing, snooping, and masquerade were used to test the model's security. The approach proved 100% successful in mitigating threats, making it acceptable for real-time healthcare applications. The suggested approach increased transmission speed by 3.5% compared to FB [4], 10.4% compared to NTM [15], and 8.5% compared to IPHL [25], making it viable for real-time clinical deployments. PoMT's use of distance measurements helps choose low-delay nodes for deployment situations. The model may be used for fast deployments.

The suggested approach reduces energy usage by 10.5% compared to FB [4], 14.6% compared to NTM [15], and 5.9% compared to IPHL [25], making it useful for high-lifetime clinical use cases. PoMT's usage of leftover node energy helps pick high-energy nodes for deployment situations. The model may be used for high-lifetime deployments. The suggested model increased throughput performance by 23.9% compared to FB [4], 19.4% compared to NTM [15], and 15.5% compared to IPHL [25], making it viable for high-data-rate deployments. PoMT's usage of temporal throughput levels helps pick high-performance nodes for deployment situations. The paradigm may be used for high-throughput installations. The suggested approach improved PDR packet consistency by 9.5% compared to FB [4], 8.3% compared to NTM [15], and 6.5% compared to IPHL [25], making it viable for high-consistency deployments. PoMT's usage of temporal PDR levels helps identify high-performance nodes for deployment situations. The paradigm may be used for high-consistency, low-data-drop deployments. These enhancements

allow real-time clinical use of the proposed model.

After being employed in clinical situations, the model's classification performance must be tested so clinicians can distinguish illness kinds and severity. The system model showed higher classification accuracy than DL [26], ABM CGC LSTM [40], and RCNN [101], making it useful for real-time clinical use cases. Combining LSTM, GRU, and RNN enhances classification accuracy. According to consistency analysis, the system model had higher classification precision than DL [26], ABM CGC LSTM [40], and RCNN [101], making it useful for consistency-aware real-time clinical use cases. Combining LSTM, GRU, and RNN enhances accuracy by extracting and classifying consistent feature sets. The system model showed greater classification recall than DL [26], ABM CGC LSTM [40], and RCNN [101], making it helpful for consistency-aware clinical use cases. Combining LSTM, GRU, and RNN, which classifies feature sets, enhances recall. In severity analysis, the system model showed 5.5% higher accuracy than DL [26], 5.4% higher accuracy than ABM CGC LSTM [40], and 2.9% higher severity than RCNN [101]. It's great for informing physicians when patients' conditions progress. Using a customized CNN helps identify severity levels from categorized sets. These improvements enable clinical scenarios requiring high QoS, speed, and security to use the proposed model.

This model's performance must be tested in real-time and may be enhanced with Generative Adversarial Networks (GANs), Q-Learning, Transformer Networks, and Auto Encoder Networks. Combining various bioinspired models may improve illness categorization and severity estimate in real-time for different use cases.

8.2 Future Work

In future study, this review may be widened to incorporate more pertinent publications and augmented with analyses of project costs, usability, and geographic issues that are inherent to Internet of Things-based applications. (IoT). Investigating the use of edge and fog computing in intelligent agriculture may be another important future research direction. This could be done as a fix for the issues that are frequently associated with centralized cloud storage systems. Massive bandwidths and high communication latencies are two issues that must be fixed. Another is the lack of support for detected events to receive real-time responses. This inquiry may lead one to the conclusion that bio-inspired and deep learning models are superior to other types of models in terms of the levels of internal efficiency they can achieve. Because of what I just said, you will encounter examples of them throughout the entirety of this thesis; don't be startled if you do. Convolutional neural network (CNN) models are used to enhance the effectiveness of feature extraction for crop type and yield prediction. The use of highly effective convolution layers, max pooling layers, ReLU layers, and dropout layers, all of which contribute to effective feature extraction, has improved performance. The model that has been supplied uses a combination of these layers to extract characteristics more effectively. To further improve the accuracy of dense layer performance, this ensemble design incorporates additional CNN models, such as VGGNet19, Xception Net, and Inception Net as well as GoogLeNet. Combining a CNN summary classifier with an incremental learning model for accuracy tweaking allows for the incremental improvement of accuracy, precision, recall, and fMeasure values. Tables 1, 2, 3, and 4 each evaluate the pertinent parameters, and Tables 5 and 6 compare these evaluations to models with high levels of efficiency to illustrate this influence. Reducing the latency with the deployment of the Yolo RCNN model enables one-iteration evaluation of the gathered data. The suggested model, which has better parametric performance compared to other deep learning models currently in use, can therefore be utilized to guarantee high efficiency in crop type recognition and yield estimate. Using long-term memory (LSTM) and gated recurrent unit (GRU) models, both of which may be further investigated with picture data, the performance of this model can be enhanced. Further analysis of this model's performance using image data is also possible. Generative adversarial networks (GANs) can be used to enhance the performance of both image and parametric data to estimate crop subtypes and yield quality for more recent soil types. The suggested model can identify agricultural production levels, disease types, and crop sowing types by

merging a variety of various deep learning algorithms, including VGGNet19, Yolo RCNN, and GWO. It can also store crop data in QoS-aware side chains. The model also makes use of a highly effective SCM layer, which, by offering a low-latency and high-security interface, helps to increase the efficiency of farmers' access. This aids the model in achieving its objective of enhancing access effectiveness. The system model was able to exhibit SCM operations with 10.5% less latency compared to VMI SCM [5], 15.4% fewer delays compared to DD SCM [12], and 12.2% fewer delays compared to RL SM [20] because to these integrations. This made it possible for the model to be used for many different high-speed use cases. Due to the usage of GWO to manage side chains, which helps SCM work better even when subjected to a range of attack types, there is a low latency. The model also showed an energy decrease of 8.5% for SCM operations in comparison to VMI SCM [5], 19.4% in comparison to DD SCM [12], and 12.8% in comparison to RL SM [20]. This makes it suitable for a wide range of low-power usage scenarios. The use of effective miner selection for SCM activities, which helps to boost SCM performance even when facing various forms of attacks, is the cause of this low consumption. The suggested model has shown crop analysis accuracy that is 8.3% higher than RL SM [20], 7.5% better than DD SCM [12], and 10.2% higher than VMI SCM [5, demonstrating that it is particularly beneficial in a variety of temporal application scenarios. This is due to the findings that the suggested model predicted. This was made possible by the use of several various deep learning algorithms, which supported ongoing improvement and increased accuracy. The suggested model outperformed VMI SCM [5], DD SCM [12], and RL SM [20] by 9.5%, 6.4%, and 6.5%, respectively. This shows that it has substantial advantages for a wide range of various real-time application scenarios. This was made possible by combining various deep learning techniques, which aided in the process of continual improvement and raised the recall level. This made it possible for it to materialize. Additionally, the system model's accuracy was 5.4% greater than RL SM [20], 8.5% better than DD SCM [12], and 9.5% better than VMI SCM [5]. Since there are so many different real-time application scenarios, it is particularly helpful in these cases. This was made possible by combining many deep learning techniques, which also helped with the continual process of raising accuracy levels and strengthening the system. The suggested model outperformed the VMI SCM [5, DD SCM [12], and RL SM [20] in terms of latency, outperforming them by 6.5%, 7.2%, and 4.8%, respectively. This makes it particularly beneficial for a variety of real-time application scenarios. This was made possible by using a variety of other deep learning techniques to aid in the process of

constant optimization and speed enhancement. For safe, quick, low-demand, high-precision, and high-precision supply chain management operations for a variety of crops, the suggested model is highly helpful. It is the end consequence of combining effective yield and crop analysis models with blockchain technology. This makes it especially beneficial for a wide range of real-time deployments. It will be important to check the model's performance for a wider variety of crops in the future. Incorporating Q-Learning and other incremental learning techniques will also improve the model's performance. Hybrid bio-inspired models can also be used to improve the model's efficiency. These models can be used in a range of farm scenarios and aim to stochastically improve accuracy and level of accuracy by carefully choosing hyperparameters.

References

[1] Fan, Linxiu. "Usage of narrowband internet of things in smart medicine and construction of robotic rehabilitation system." *IEEE Access* 10 (2021): 6246-6259.

[2] Cuzzocrea, Alfredo, Ladjel Bellatreche, and Il-Yeol Song. "Data warehousing and OLAP over big data: current challenges and future research directions." In *Proceedings of the sixteenth international workshop on Data warehousing and OLAP*, pp. 67-70. 2013.

[3] Raj, Pethuru, Jyotir Moy Chatterjee, Abhishek Kumar, and B. Balamurugan, eds. “Internet of things use cases for the healthcare industry.” *Springer*, 2020.,

[4] Pattnaik, Prasant Kumar, Suneeta Mohanty, and Satarupa Mohanty, eds. "Smart Healthcare Analytics in IoT Enabled Environment.” *Springer,* 2020.

[5] Chakraborty, Chinmay, Amit Banerjee, Maheshkumar H. Kolekar, Lalit Garg, and Basabi Chakraborty, eds. “Internet of things for healthcare technologies.” *Springer*, 2021.

[6] Gupta, Nishu, and Sara Paiva, eds.” IoT and ICT for Healthcare Applications.” Cham, Switzerland: *Springer*, 2020.

[7] Dash, Satya Prakash. "The impact of IoT in healthcare: global technological change & the roadmap to a networked architecture in India." *Journal of the Indian Institute of Science* 100, no. 4 (2020): 773-785.

[8] Bhatia, Harshita, Surya Narayan Panda, and Dimple Nagpal. "Internet of Things and its Applications in Healthcare-A Survey." In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 305-310. IEEE, 2020.

[9] Amin, Syed Umar, and M. Shamim Hossain. "Edge intelligence and Internet of Things in healthcare: A survey." *IEEE Access* 9 (2020): 45-59.

[10] Kadhim, Kadhim Takleef, Ali M. Alsahlany, Salim Muhsin Wadi, and Hussein T. Kadhum. "An overview of patient's health status monitoring system based on internet of things (IoT)." *Wireless Personal Communications* 114, no. 3 (2020): 2235-2262.

[11] Malik, Nikita, and Sanjay Kumar Malik. "Using IoT and semantic web technologies for healthcare and medical sector." *Ontology-Based Information Retrieval for Healthcare Systems* (2020): 91-115.

[12] Arulanthu, Pramila, and Eswaran Perumal. "An intelligent IoT with cloud centric medical decision support system for chronic kidney disease prediction." *International Journal of Imaging Systems and Technology* 30, no. 3 (2020): 815-827.

[13] Liyanage, Madhusanka, An Braeken, Pardeep Kumar, and Mika Ylianttila, eds. "IoT security: Advances in authentication." *John Wiley & Sons*, 2020.

[14] Deebak, B. D., and Fadi Al-Turjman. "Secure-user sign-in authentication for IoT-based eHealth systems." *Complex & Intelligent Systems* (2021): 1-21.

[15] Badawy, Mahmoud M., Zainab H. Ali, and Hesham A. Ali. "QoS provisioning framework for service-oriented internet of things (IoT)." *Cluster Computing* 23 (2020): 575-591.

[16] Singh, Manisha, Gaurav Baranwal, and Anil Kumar Tripathi. "QoS-aware selection of IoT-based service." *Arabian Journal for Science and Engineering* 45, no. 12 (2020): 10033-10050.

[17] Selvakanmani, S., and M. Sumathi. "Fuzzy assisted fog and cloud computing with MIoT system for performance analysis of health surveillance system." *Journal of Ambient Intelligence and Humanized Computing* 12 (2021): 3423-3436.

[18] Krishna, P. Venkata, Sasikumar Gurumoorthy, and Mohammad S. Obaidat. "Internet of things and personalized healthcare systems." *Springer*, Singapore, 2019.

[19] El Kafhali, Said, and Khaled Salah. "Performance modelling and analysis of Internet of Things enabled healthcare monitoring systems." *IET Networks* 8, no. 1 (2019): 48-58.

[20] Yang, Xin, Shah Nazir, Habib Ullah Khan, Muhammad Shafiq, and Neelam Mukhtar. "Parallel computing for efficient and intelligent industrial internet of health things: an overview." *Complexity* 2021 (2021): 1-11.

[21] Islam, SM Riazul, Daehan Kwak, MD Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. "The internet of things for health care: a comprehensive survey." *IEEE access* 3 (2015): 678-708.

[22] Hong, Zicong, Wuhui Chen, Huawei Huang, Song Guo, and Zibin Zheng. "Multi-hop cooperative computation offloading for industrial IoT–edge–cloud computing environments." *IEEE Transactions on Parallel and Distributed Systems* 30, no. 12 (2019): 2759-2774.

[23] Zhang, Naiheng. "Service discovery and selection based on dynamic qos in the internet of things." *Complexity 2021* (2021): 1-12.

[24] Cao, Kun, Guo Xu, Junlong Zhou, Tongquan Wei, Mingsong Chen, and Shiyan Hu. "QoS-adaptive approximate real-time computation for mobility-aware IoT lifetime optimization." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 38, no. 10 (2018): 1799-1810.

[25] Habibzadeh, Hadi, Karthik Dinesh, Omid Rajabi Shishvan, Andrew Boggio-Dandry, Gaurav Sharma, and Tolga Soyata. "A survey of healthcare Internet of Things (HIoT): A clinical perspective." *IEEE Internet of Things Journal* 7, no. 1 (2019): 53-71.

[26] Liu, Yinqiu, Kun Wang, Kai Qian, Miao Du, and Song Guo. "Tornado: Enabling blockchain in heterogeneous Internet of Things through a space-structured approach." *IEEE Internet of Things Journal* 7, no. 2 (2019): 1273-1286.

[27] Zhou, Xiaokang, Wei Liang, I. Kevin, Kai Wang, Hao Wang, Laurence T. Yang, and Qun Jin. "Deep-learning-enhanced human activity recognition for Internet of healthcare things." *IEEE Internet of Things Journal* 7, no. 7 (2020): 6429-6438.

[28] Shim, Kyung-Ah. "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things." *IEEE Internet of Things Journal* 6, no. 5 (2019): 9211-9212.

[29] Kumar, Mahender, and Satish Chand. "A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability.*" IEEE Internet of Things Journal* 7, no. 10 (2020): 10650-10659.

[30] Kumar, Adarsh, Rajalakshmi Krishnamurthi, Anand Nayyar, Kriti Sharma, Vinay Grover, and Eklas Hossain. "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes." *IEEE access* 8 (2020): 118433-118471.

[31] Ray, Partha Pratim, Dinesh Dash, Khaled Salah, and Neeraj Kumar. "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases." *IEEE Systems Journal* 15, no. 1 (2020): 85-94.

[32] Khatri, Sabita, Fahad Ahmed Alzahrani, Md Tarique Jamal Ansari, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "A systematic analysis on blockchain integration with healthcare domain: scope and challenges." *IEEE Access* 9 (2021): 84666-84687.

[33] Zarour, Mohammad, Md Tarique Jamal Ansari, Mamdouh Alenezi, Amal Krishna Sarkar, Mohd Faizan, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records." *IEEE Access* 8 (2020): 157959-157973.

[34] Mazlan, Ahmad Akmaluddin, Salwani Mohd Daud, Suriani Mohd Sam, Hafiza Abas, Siti Zaleha Abdul Rasid, and Muhammad Fathi Yusof. "Scalability challenges in healthcare blockchain system—a systematic review." *IEEE Access* 8 (2020): 23663-23673.

[35] Ren, Junyu, Jinze Li, Huaxing Liu, and Tuanfa Qin. "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT." *Tsinghua Science and Technology* 27, no. 4 (2021): 760-776.

[36] Omar, Ilhaam A., Raja Jayaraman, Mazin S. Debe, Khaled Salah, Ibrar Yaqoob, and Mohammed Omar. "Automating procurement contracts in the healthcare supply chain using blockchain smart contracts." *IEEE Access* 9 (2021): 37397-37409.

[37] Subramanian, Ganesan, and Anand Sreekantan Thampy. "Implementation of blockchain consortium to prioritize diabetes patients' healthcare in pandemic situations." *IEEE Access* 9 (2021): 162459-162475.

[38] Abdellatif, Alaa Awad, Lutfi Samara, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, Mohsen Guizani, Mark Dennis O'Connor, and James Laughton. "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15762-15775.

[39] Gupta, Brij B., Kuan-Ching Li, Victor CM Leung, Kostas E. Psannis, and Shingo Yamaguchi. "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system." *IEEE/CAA Journal of Automatica Sinica* 8, no. 12 (2021): 1877-1890.

[40] Chinaei, Mohammad Hossein, Hassan Habibi Gharakheili, and Vijay Sivaraman. "Optimal witnessing of healthcare IoT data using blockchain logging contract." *IEEE Internet of Things Journal* 8, no. 12 (2021): 10117-10130.

[41] Iqbal, Mubashar, and Raimundas Matulevičius. "Exploring sybil and double-spending risks in blockchain systems." *IEEE Access* 9 (2021): 76153-76177.

[42] Bhattacharya, Pronaya, Sudeep Tanwar, Umesh Bodkhe, Sudhanshu Tyagi, and Neeraj Kumar. "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications." *IEEE transactions on network science and engineering* 8, no. 2 (2019): 1242-1255.

[43] Kassab, Mohamad, Joanna DeFranco, Tarek Malas, Phillip Laplante, Giuseppe Destefanis, and Valdemar Vicente Graciano Neto. "Exploring research in blockchain for healthcare and a roadmap for the future." *IEEE Transactions on Emerging Topics in* Computing 9, no. 4 (2019): 1835-1852.

[44] Li, Peilong, Chen Xu, Hao Jin, Chunyang Hu, Yan Luo, Yu Cao, Jomol Mathew, and Yunsheng Ma. "ChainSDI: a software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains." *IEEE Systems Journal* 14, no. 2 (2019): 2042-2053.

[45] Singh, Akhilendra Pratap, Nihar Ranjan Pradhan, Ashish K. Luhach, Sivansu Agnihotri, Noor Zaman Jhanjhi, Sahil Verma, Uttam Ghosh, and Diptendu Sinha Roy. "A novel patient-centric architectural framework for blockchain-enabled healthcare applications." *IEEE Transactions on Industrial Informatics* 17, no. 8 (2020): 5779-5789.

[46] Ismail, Leila, Huned Materwala, and Sherali Zeadally. "Lightweight blockchain for healthcare." *IEEE Access* 7 (2019): 149935-149951.

[47] Ray, Partha Pratim, Biky Chowhan, Neeraj Kumar, and Ahmad Almogren. "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem." *IEEE Internet of Things Journal* 8, no. 13 (2021): 10857-10872.

[48] Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "Bedgehealth: A decentralized architecture for edge-based iomt networks using blockchain." *IEEE Internet of Things Journal* 8, no. 14 (2021): 11743-11757.

[49] Saini, Akanksha, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, and Yushu Zhang. "A smart-contract-based access control framework for cloud smart healthcare system." *IEEE Internet of Things Journal* 8, no. 7 (2020): 5914-5925.

[50] Lee, Deoksang, and Minseok Song. "MEXchange: A privacy-preserving blockchain-based framework for health information exchange using ring signature and stealth address." *IEEE Access* 9 (2021): 158122-158139.

[51] [Aujla, Gagangeet Singh, and Anish Jindal. "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring." *IEEE Journal on Selected Areas in Communications* 39, no. 2 (2020): 491-499.

[52] Bao, Zijian, Qinghao Wang, Wenbo Shi, Lei Wang, Hong Lei, and Bangdao Chen. "When blockchain meets sgx: An overview, challenges, and open issues." *IEEE Access* 8 (2020): 170404-170420.

[53] Jolfaei, Amirhossein Adavoudi, Seyed Farhad Aghili, and Dave Singelee. "A survey on blockchain-based IoMT systems: Towards scalability." *IEEE Access* 9 (2021): 148948-148975.

[54] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." *IEEE Internet of Things Journal* 8, no. 14 (2021): 11717-11731.

[55] Masud, Mehedi, Gurjot Singh Gaba, Salman Alqahtani, Ghulam Muhammad, Brij B. Gupta, Pardeep Kumar, and Ahmed Ghoneim. "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care." *IEEE Internet of Things Journal* 8, no. 21 (2020): 15694-15703.

[56] Meng, Weizhi, Yong Cai, Laurence T. Yang, and Wei-Yang Chiu. "Hybrid emotion-aware monitoring system based on brainwaves for internet of medical things." *IEEE Internet of Things Journal* 8, no. 21 (2021): 16014-16022.

[57] Sun, Jiangfeng, Fazlullah Khan, Junxia Li, Mohammad Dahman Alshehri, Ryan Alturki, and Mohammad Wedyan. "Mutual authentication scheme for the device-to-server communication in the Internet of medical things." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15663-15671.

[58] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a block chain-based framework for security and privacy-assured internet of medical things with effective access control." *IEEE Internet of Things Journal* 8, no. 14 (2021): 11717-11731.

[59] Mao, Yi, and Lei Zhang. "Optimization of the medical service consultation system based on the artificial intelligence of the internet of things." *IEEE Access* 9 (2021): 98261-98274.

[60] Ding, Yi, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin. "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things." *IEEE Internet of Things Journal* 8, no. 3 (2020): 1504-1518.

[61] Xu, Chenchu, Zhifan Gao, Dong Zhang, Jinglin Zhang, Lei Xu, and Shuo Li. "Applying cross-modality data processing for infarction learning in medical internet of things." *IEEE Internet of Things Journal* 8, no. 23 (2021): 16902-16910.

[62] Shah, Syed Hassan Ahmed, Deepika Koundal, Vyasa Sai, and Shalli Rani. "Guest Editorial: Special section on 5G edge computing-enabled internet of medical things." *IEEE Transactions on Industrial Informatics* 18, no. 12 (2022): 8860-8863.

[63] Yang, Fan, Qilu Wu, Xiping Hu, Jiancong Ye, Yuting Yang, Haocong Rao, Rong Ma, and Bin Hu. "Internet-of-Things-enabled data fusion method for sleep healthcare applications." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15892-15905.

[64] [Jia, Licheng, Lei Shi, Chongbin Liu, Jing Xu, Yongjie Gao, Chengliang Sun, Sheng Liu, and Guoqiang Wu. "Piezoelectric micromachined ultrasonic transducer array-based electronic stethoscope for internet of medical things." *IEEE Internet of Things Journal* 9, no. 12 (2022): 9766-9774.

[65] Wu, Guangjun, Shupeng Wang, and Zhaolong Ning. "Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things." *IEEE Internet of Things Journal* 9, no. 11 (2021): 8091-8104.

[66] Zeng, Peng, Zhiting Zhang, Rongxing Lu, and Kim-Kwang Raymond Choo. "Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things." *IEEE Internet of Things Journal* 8, no. 13 (2021): 10963-10972.

[67] Su, Yu-Sheng, Ting-Jou Ding, and Mu-Yen Chen. "Deep learning methods in internet of medical things for valvular heart disease screening system." *IEEE Internet of Things Journal* 8, no. 23 (2021): 16921-16932.

[68] Gleim, Lars, Jan Pennekamp, Martin Liebenberg, Melanie Buchsbaum, Philipp Niemietz, Simon Knape, Alexander Epple et al. "FactDAG: formalizing data interoperability in an internet of production." *IEEE Internet of Things Journal* 7, no. 4 (2020): 3243-3253.

[69] Awan, Kamran Ahmad, Ikram Ud Din, Ahmad Almogren, Hisham Almajed, Irfan Mohiuddin, and Mohsen Guizani. "NeuroTrust—Artificial-Neural-Network-Based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things." *IEEE Internet of Things Journal* 8, no. 21 (2020): 15672-15682.

[70] Magdy, Mahmoud, Neveen I. Ghali, Said Ghoniemy, and Khalid M. Hosny. "Multiple Zero-Watermarking of Medical Images for Internet of Medical Things." *IEEE Access* 10 (2022): 38821-38831.

[71] Yan, Fei, Hesheng Huang, and Xu Yu. "A Multiwatermarking Scheme for Verifying Medical Image Integrity and Authenticity in the Internet of Medical Things." *IEEE Transactions on Industrial Informatics* 18, no. 12 (2022): 8885-8894.

[72] Almogren, Ahmad, Irfan Mohiuddin, Ikram Ud Din, Hisham Almajed, and Nadra Guizani. "Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things." *IEEE Internet of Things Journal* 8, no. 6 (2020): 4485-4497.

[73] Manogaran, Gunasekaran, Mamoun Alazab, Houbing Song, and Neeraj Kumar. "CDP-UA: Cognitive data processing method wearable sensor data uncertainty analysis in the internet of things assisted smart medical healthcare systems." *IEEE Journal of Biomedical and Health Informatics* 25, no. 10 (2021): 3691-3699.

[74] Lin, Hui, Sahil Garg, Jia Hu, Xiaoding Wang, Md Jalil Piran, and M. Shamim Hossain. "Privacy-enhanced data fusion for COVID-19 applications in intelligent

Internet of medical Things." *IEEE Internet of Things Journal* 8, no. 21 (2020): 15683-15693.

[75] Chen, Jie, Xiaoxiao Song, Zhichao Huang, Jianqiang Li, Zhaoxia Wang, Chengwen Luo, and Fei Yu. "On-Site Colonoscopy Autodiagnosis Using Smart Internet of Medical Things." *IEEE Internet of Things Journal* 9, no. 11 (2021): 8657-8668.

[76] Alshehri, Fatima, and Ghulam Muhammad. "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare." *IEEE Access* 9 (2020): 3660-3678.

[77] Gopikrishnan, S., P. Priakanth, Gautam Srivastava, and Giancarlo Fortino. "EWPS: Emergency data communication in the Internet of Medical Things." *IEEE Internet of Things Journal* 8, no. 14 (2021): 11345-11356.

[78] Zhang, Tao, Minjie Liu, Tian Yuan, and Najla Al-Nabhan. "Emotion-aware and intelligent internet of medical things toward emotion recognition during COVID-19 pandemic." *IEEE Internet of Things Journal* 8, no. 21 (2020): 16002-16013.

[79] Bigini, Gioele, and Emanuele Lattanzi. "Toward the InterPlanetary Health Layer for the Internet of Medical Things With Distributed Ledgers and Storages." *IEEE Access* 10 (2022): 82883-82895.

[80] Saheed, Yakub Kayode, and Micheal Olaolu Arowolo. "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms." *IEEE Access* 9 (2021): 161546-161554.

[81] Zhang, Peng, Yanwen Hang, Xiaomiao Ye, Ping Guan, Jun Jiang, Jiancheng Tan, and Wei Hu. "A United CNN-LSTM algorithm combining RR wave signals to detect arrhythmia in the 5G-enabled medical internet of things." *IEEE Internet of Things Journal* 9, no. 16 (2021): 14563-14571.

[82] Lee, Tian-Fu, Xiucai Ye, and Syuan-Han Lin. "Anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things." *IEEE Internet of Things Journal* 9, no. 16 (2022): 15336-15348.

[83] Hasan, Mohammad Kamrul, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." *IEEE Access* 9 (2021): 47731-47742.

[84] Silva, Francisco Airton, Tuan Anh Nguyen, Iure Fé, Carlos Brito, Dugki Min, and Jae-Woo Lee. "Performance evaluation of an internet of healthcare things for medical monitoring using M/M/c/K queuing models." *IEEE Access* 9 (2021): 55271-55283.

[85] Wang, Wei, Fang Liu, Xiaohui Zhi, Tong Zhang, and Chuanchao Huang. "An integrated deep learning algorithm for detecting lung nodules with low-dose ct and its application in 6g-enabled internet of medical things." *IEEE Internet of Things Journal* 8, no. 7 (2020): 5274-5284.

[86] Saha, Rahul, Gulshan Kumar, Neeraj Kumar, Tai-Hoon Kim, Tannishtha Devgun, Reji Thomas, and Ahmed Barnawi. "Internet of things framework for oxygen saturation monitoring in COVID-19 environment." *IEEE Internet of Things Journal* 9, no. 5 (2021): 3631-3641.

[87] Demirel, Berken Utku, Islam Abdelsalam Bayoumy, and Mohammad Abdullah Al Faruque. "Energy-efficient real-time heart monitoring on edge–fog–cloud internet of medical things." *IEEE Internet of Things Journal* 9, no. 14 (2021): 12472-12481.

[88] Deebak, Bakkiam David, and Fadi Al-Turjman. "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things." *IEEE Journal on Selected Areas in Communications* 39, no. 2 (2020): 346-360.

[89] Manogaran, Gunasekaran, Gautam Srivastava, Bala Anand Muthu, S. Baskar, P. Mohamed Shakeel, Ching-Hsien Hsu, Ali Kashif Bashir, and Priyan M. Kumar. "A response-aware traffic offloading scheme using regression machine learning for user-centric large-scale internet of things." *IEEE Internet of Things Journal* 8, no. 5 (2020): 3360-3368.

[90] Rahman, Md Abdur, and M. Shamim Hossain. "An internet-of-medical-things-enabled edge computing framework for tackling COVID-19." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15847-15854.

[91] Abdellatif, Alaa Awad, Lutfi Samara, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, Mohsen Guizani, Mark Dennis O'Connor, and James Laughton. "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15762-15775.

[92] Kakhi, Kourosh, Roohallah Alizadehsani, HM Dipu Kabir, Abbas Khosravi, Saeid Nahavandi, and U. Rajendra Acharya. "The internet of medical things and artificial intelligence: trends, challenges, and opportunities." *Biocybernetics and Biomedical Engineering* (2022).

[93] Zhan, Yu, Baocang Wang, and Rongxing Lu. "Cryptanalysis and improvement of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks." IEEE Internet of Things Journal 8, no. 7 (2020): 5973-5984.

[94] Xu, Shihao, Haocong Rao, Hong Peng, Xin Jiang, Yi Guo, Xiping Hu, and Bin Hu. "Attention-based multilevel co-occurrence graph convolutional LSTM for 3-D action recognition." *IEEE Internet of Things Journal* 8, no. 21 (2020): 15990-16001.

[95] Parah, Shabir A., Javaid A. Kaw, Paolo Bellavista, Nazir A. Loan, Ghulam Mohiuddin Bhat, Khan Muhammad, and Victor Hugo C. de Albuquerque. "Efficient security and authentication for edge-based internet of medical things." IEEE Internet of Things Journal 8, no. 21 (2020): 15652-15662.

[96] Nguyen, Tuan Anh, Dugki Min, Eunmi Choi, and Jae-Woo Lee. "Dependability and security quantification of an internet of medical things infrastructure based on cloud-fog-edge continuum for healthcare monitoring using hierarchical models." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15704-15748.

[97] Cai, Hanshu, Yi Zhang, Han Xiao, Jian Zhang, Bin Hu, and Xiping Hu. "An adaptive neurofeedback method for attention regulation based on the internet of things." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15829-15838.

[98] Li, Jiliang, Zhou Su, Deke Guo, Kim-Kwang Raymond Choo, and Yusheng Ji. "PSL-MAAKA: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things." *IEEE Internet of Things Journal* 8, no. 17 (2021): 13183-13195.

[99] Jin, Hai, Xiaohai Dai, Jiang Xiao, Baochun Li, Huichuwu Li, and Yan Zhang. "Cross-cluster federated learning and blockchain for internet of medical things." *IEEE Internet of Things Journal* 8, no. 21 (2021): 15776-15784.

[100] Kumar, Priyan Malarvizhi, Choong Seon Hong, Fatemeh Afghah, Gunasekaran Manogaran, Keping Yu, Qiaozhi Hua, and Jiechao Gao. "Clouds proportionate medical data stream analytics for internet of things-based healthcare systems." *IEEE Journal of Biomedical and Health Informatics* 26, no. 3 (2021): 973-982.

[101] Ning, Wenlong, Shuhua Li, Dongmei Wei, Long Zhe Guo, and Hong Chen. "Automatic detection of congestive heart failure based on a hybrid deep learning algorithm in the internet of medical things." *IEEE Internet of Things Journal* 8, no. 16 (2020): 12550-12558.

[102] Li, Hang, Keping Yu, Bin Liu, Chaosheng Feng, Zhiguang Qin, and Gautam Srivastava. "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things." *IEEE Journal of Biomedical and Health Informatics* 26, no. 5 (2021): 1949-1960.

[103] Bhuiyan, Mohammad Nuruzzaman, Md Mahbubur Rahman, Md Masum Billah, and Dipanita Saha. "Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities." *IEEE Internet of Things Journal* 8, no. 13 (2021): 10474-10498.

Appendix I

List of Publications

1. **Mrs. Pooja Mishra, Dr. Sandeep Malik,** "QSIH: Design of a Novel QoS-Aware Sidechain-Based IoT Network Design for Secure Healthcare Deployments", International Journal of Computer Networks and Applications (IJCNA) ,ISSN :2395-0455 Volume 9, Issue 5, 2022, 624– 640.

2. **Mrs. Pooja Mishra, Dr. Sandeep Malik,** "Improving the Effectiveness Of IoT-Based Healthcare Monitoring and Control Devices using Deep Learning Models" TELEMATIQUE, ISSN: 1856-4194, Volume 21 Issue 1, 2022, 5569 – 5593.

3. **Mrs. Pooja Mishra, Dr. Sandeep Malik**, "Systematic Review of Health Monitoring System using the Internet of Things (IoT)", International Journal of Future Generation Communication and Networking(IFGCN), ISSN:2233-7857, Vol. 13, No. 4, (2020), pp. 4927–4941 ©2020 SERSC

4. **Ms. Pooja Mishra, Dr. Sandeep Malik,** "BDSIHD: Design of a Blockchain-powered Deep transfer learning-based highly Secure IoMT data processing model for Healthcare Deployments", to International Journal of Computers and Applications- Accepted.

Appendix II

Published Research Papers

[1] QSIH: Design of a Novel QoS-Aware Sidechain-Based IoT Network Design for Secure Healthcare Deployments, International Journal of Computer Networks and Applications (IJCNA)

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/215921 Volume 9, Issue 5, September – October (2022)

RESEARCH ARTICLE

QSIH: Design of a Novel QoS-Aware Sidechain-Based IoT Network Design for Secure Healthcare Deployments

Pooja Mishra
Department of Computer Science and Engineering, Oriental University, Indore, Madhya Pradesh, India.
pooja26.mishra@gmail.com

Sandeep Malik
Department of Computer Science and Engineering, Oriental University, Indore, Madhya Pradesh, India.
sandeepmalik@orientaluniversity.in

Received: 17 August 2022 / Revised: 11October 2022 / Accepted: 15 October 2022 / Published: 30 October 2022

Abstract – Internet of Medical Things (IoMT) are networks which are targeted towards design of healthcare communication interfaces with low latency and high security. In order to design such interfaces, efficient models for data encryption, hashing, privacy, and quality of service (QoS) awareness are needed. A wide variety of standard medical interfaces are proposed by researchers, which assist in reducing network redundancies for high-throughput and low latency communications. These interfaces also implement security models that ensure data encryption & privacy. But due to incorporation of encryption methods, QoS performance of the IoMT devices reduces, which limits their real-time usability for in-patient monitoring & treatment. In order to improve IoMT QoS while maintaining high security, this text proposes design of QSIH, which is a QoS-aware sidechain model that can be used for securing IoMT networks. The proposed model describes design of a blockchain-based data storage & communication interface, which is capable of removing a wide variety of network attacks. The delay needed for communication in any blockchain-based interface increases exponentially w.r.t. number of blocks added to the system. In order to reduce this delay, a novel machine learning model based on Genetic Algorithm optimization is proposed. The proposed model splits the main blockchain into multiple shards in a QoS-aware manner, thereby ensuring low delay, and high communication throughput. The shards (or sidechains) are managed using an interactive Q-Learning (IQL), which is able to expand or contract these chains depending upon network's QoS performance. Sidechains which are unused for large periods of time are combined together, and archived for future reference. The archived sidechains are formed from main blockchain, and are merged with other sidechains depending upon archival requirements of the network. Due to such a dynamic side chaining model, the proposed QSIH model is capable of reducing network communication delay by 18%, increase throughput by 14%, reduce storage cost by 5%, while maintaining high level of security & privacy in the network. The model was tested under different IoMT scenarios, and it was observed that it showcased consistent performance across different network emulations.

Index Terms – IoMT, Healthcare, Blockchain, Machine Learning, Sidechain, Optimization, QoS.

1. INTRODUCTION

In order to perform high speed, high accuracy, and high performance IoT based health care monitoring, the designed devices must follow certain principles. These principles include high precision monitoring, effective analysis, and efficient control. A large number of algorithms have been proposed for performing these tasks, and each of the algorithms have their own nuances, advantages, and limitations. But in order to understand the process of data flow in healthcare IoT, it is necessary that IoT components like sensors, storage devices, analytical processing algorithms, cloud deployments, and actuation points must be carefully studied. The flow of a typical healthcare IoT model [1], that includes sensors, storage devices, analytical processing units, cloud interface and actuating entities (Doctors) can be observed from figure 1, wherein flow of data from devices to storage, and back to reporting can be observed. Any healthcare IoT system works in the following steps,

- Data capturing from wearable and non-wearable devices, wherein data from ECG sensors, blood pressure sensors, oxygen monitors, and temperature monitors, etc. is captured and stored into a unified format. This data is then given to the cloud for further processing. There are 2 main responsibilities of every data capture IoT healthcare device.
  - Reduce any reading errors during data capturing, which is done via pre-processing algorithms like adaptive median filtering, averaging, etc.

[2] Improving the Effectiveness Of IoT-Based Healthcare Monitoring and Control

Devices using Deep Learning Models, TELEMATIQUE

TELEMATIQUE
ISSN: 1856-4194

Volume 21 Issue 1, 2022
5569 – 5593

Improving the Effectiveness Of Iot-Based Healthcare Monitoring and Control Devices using Deep Learning Models

Ms. Pooja Mishra[1], Dr. Sandeep Malik[2]

[1]Research Scholar, Department of CSE, Oriental University, Indore MP (INDIA).
[2]Professor, Department of CSE, Oriental University, Indore MP (INDIA)

Received 05/09/2022; **Accepted** 28/09/2022

Abstract:

Internet of Things (IoT) is a boon to the healthcare industry, which is due to its inherent advantages like ability of remote monitoring, remote actuation, high speed data processing and low operation costs. IoT devices like electrocardiogram (ECG) monitor, continuous blood pressure (CBP) monitor, continuous oxygen level monitor, etc. are being used by Doctors worldwide to effectively monitor patient conditions and reduce overheads on the currently overloaded nursing staff. Due to high availability of computational resources and limited power constraints at hospitals and other healthcare stations, IoT devices can step up their performance via high accuracy temporal data analysis and decision making in case of even the slightest of anomalies. Some of the newer IoT systems have implemented such high accuracy algorithms for improving their applicability in real time monitoring & control. But the older systems need to be replaced to upgrade their performance, which raises a lot of issues, including but not limited to cost of replacement, calibration, familiarity of nursing staff with old equipment, etc. To reduce the effect of these issues this chapter proposes a novel high accuracy, highly interfaceable, and low cost deep learning solution, which can be integrated with both old and new healthcare monitoring devices to improve their efficiency. Certain minimum application criteria are defined for a device to be eligible for interfacing, and it is observed that more than 80% of currently working healthcare devices can be upgraded via this architecture, and their effectiveness of monitoring & control can be improved. The proposed architecture is found to be more than 99% accurate in terms of parameter monitoring, and has excellent control exercising capabilities.

Keywords: Healthcare, IoT, machine learning, deep learning, interface

1. INTRODUCTION

In order to perform high speed, high accuracy, and high performance IoT based health care monitoring, the designed devices must follow certain principles. These principles include high precision monitoring, effective analysis, and efficient control. A large number of algorithms have been proposed for performing these tasks, and each of the algorithms have their own nuances, advantages, and limitations. But in order to understand the process of data flow in healthcare IoT, it is necessary that IoT components like sensors, storage devices, analytical processing algorithms, cloud deployments, and actuation points must be carefully studied. The flow of a typical healthcare IoT system, that includes sensors, storage devices, analytical processing units, cloud interface and actuating entities (Doctors) can be observed

[3] Systematic Review of Health Monitoring System using the Internet of Things (IoT), International Journal of Future Generation Communication and Networking(IFGCN)

International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4927–4941

Systematic Review of Health Monitoring System using the Internet of Things (IoT)

Pooja Mishra, Dr. Sandeep Malik
Computer Science and Engineering Department, Oriental University, Indore, MP,
Computer Science and Engineering Department, Oriental University, Indore, MP,
pooja26.mishra@gmail.com , sandeepmalik@orientaluniversity.inE-mail

Abstract

The challenges of health and social care are explicitly reflected by the increasing environmental levels. Technology-dependent livelihoods have become investigators' focal point. In order to solve these healthcare issues, technology has played a crucial role in completing these important tasks. While using technological solutions, expert advice must be used to design , implement and validate them. There is a genuine need for healthcare expenses to be regulated or even reduced while enhancing service quality. The real-time monitoring of the health status of the body organ may be used to assess the health status of a specific organ in order to resolve these challenges; therefore, it would be possible to enable early provision of medical facilities. The technology used in this paper focuses on the ability to concentrate on the physiological data of a person to detect the health of body organs, which may help cure defects. This is done by correctly processing and assessing the collected data from sensors when transmitting health status detection. It supports the finding of organ health status that will facilitate clinical decision-making to provide care.

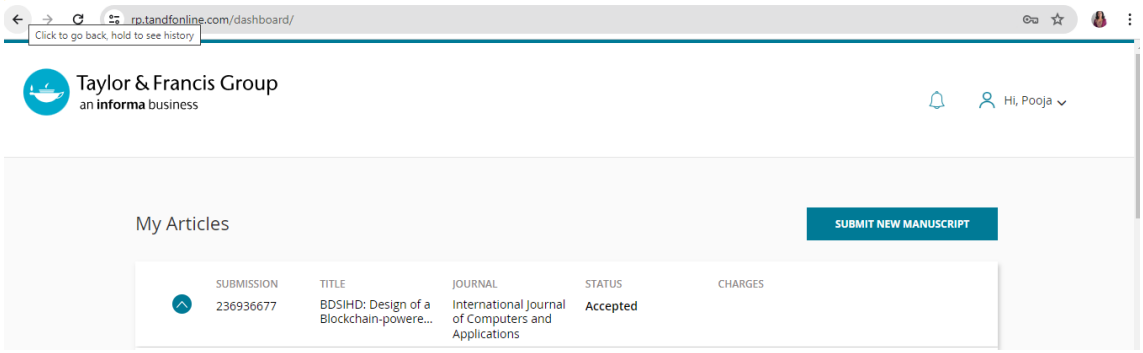
Keywords: *Internet of things, Healthcare, Medical ,Real-time monitoring, Wireless sensor networks*

1. Introduction

In this paper, using the IoT, we monitor various parameters related to patient health. In the IoT paper-based patient health tracking system, the real-time parameters of the health of a patient are submitted to the cloud using Internet connectivity. These parameters are sent to a remote location on the Internet so that the user can access these data, regardless of geographical location, from anywhere. However, by combining various technologies, such as Android phone apps, wearable devices and sensors, the caregiver of a patient can be remotely monitored easily. Healthcare providers are more often visited in our busy lifestyle to meet individual needs, since the enormous population increase leads to more customers in our new and static healthcare systems. On the other hand, there is still insufficient investment in healthcare in new technology to manage these populations. In addition, we are significantly concerned about our health and interested in continuously monitoring our physical activity everywhere at any time using different healthcare and fitness tracking products, similar to other individuals. Moreover, as we do our day-to-day work, when we leave them home alone for a long time, we worry about our wounded family member and disabled people's welfare. Therefore, in order to provide a secure and convenient world for all to live in, it is becoming important to engage innovations such as healthcare sensors and wearables with our healthcare systems. The growing population, followed by the prevalence of ageing-related chronic diseases, would have significant consequences for decades to come for the health care system. Therefore, we suggest a model that allows continuous real-time observation of health of elderly people to prevent chronic diseases, thus avoiding hospitalization that burdens healthcare systems and costs. This paper provides a system for Health Tracking using the Internet of Things. The machine accumulates physiological data from patients in real-time via

ISSN: 2233-7857 IJFGCN

[4] BDSIHD: Design of a Blockchain-powered Deep transfer learning-based highly Secure IoMT data processing model for Healthcare Deployments", to International Journal of Computers and Applications- Paper Accepted



Appendix III

Plagiarism Report

Mishra_Pooja_Thesis

ORIGINALITY REPORT

10%	8%	4%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	mail.ijcna.org Internet Source	6%
2	orca.cardiff.ac.uk Internet Source	1%
3	Hemlata Kohad, Sunil Kumar, Asha Ambhaikar. "Scalability of Blockchain based E-voting system using Multiobjective Genetic Algorithm with Sharding", 2022 IEEE Delhi Section Conference (DELCON), 2022 Publication	<1%
4	"Decision Analytics for Sustainable Development in Smart Society 5.0", Springer Science and Business Media LLC, 2022 Publication	<1%
5	Hoa Hong Nguyen, Farhaan Mirza, M. Asif	<1%