A Power-Aware IoT-Fog-Cloud Architecture for Telehealth Applications

by

Yunyong Guo
B.Sc., University of NanKai, 2000
M.A., University of Victoria, 2012

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Computer Science

We acknowledge and respect the Lək̓ʷəŋən (Songhees and Xʷsepsəm/Esquimalt)
Peoples on whose territory the university stands, and the Lək̓ʷəŋən and W̱SÁNEĆ
Peoples whose historical relationships with the land continue to this day.

A Power-Aware IoT-Fog-Cloud Architecture for Telehealth Applications

by

Yunyong Guo
B.Sc., University of NanKai, 2000
M.A., University of Victoria, 2012

Supervisory Committee

Prof. Sudhakar Ganti, Supervisor
(Department of Computer Science)

Prof. Kui Wu, Departmental Member
(Department of Computer Science)

Prof. Alex Kuo, Outside Member
(Department of Health Information Science)

ABSTRACT

This dissertation presents an energy-efficient model for integrating Internet of Things (IoT) devices with fog and cloud computing platforms, specifically designed for telehealth applications. As the deployment of telehealth IoT devices continues to grow, the demand for efficient, real-time data processing and energy conservation becomes increasingly critical. This research addresses these challenges by proposing a hybrid architecture that combines the low-latency benefits of fog computing with the scalable resources of cloud computing. The model reduces energy consumption by processing data locally through fog nodes, minimizing the need for constant communication with cloud servers. This not only decreases latency but also optimizes the use of computational resources, making the system more adaptable to the dynamic demands of telehealth services. The model is further enhanced by an adaptive resource scaling algorithm, which dynamically adjusts processing capacity based on workload, ensuring both efficiency and reliability in critical healthcare applications. Simulations studies demonstrate the effectiveness of the model in reducing energy consumption and improving system performance for real-time telehealth monitoring. The results show significant improvements in data processing speed, energy efficiency, and resource utilization compared to traditional cloud-only architectures. This work contributes to the ongoing development of sustainable telehealth solutions by providing a robust framework for IoT-fog-cloud integration that meets the stringent demands of modern healthcare systems.

Contents

Declaration of Authorship

I, Yunyong Guo, declare that this proposal titled, "A Power-Aware IoT-Fog-Cloud Architecture for Telehealth Applications" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. Except for such quotations, this proposal is entirely my own work.
- I have acknowledged all the main sources of help.

List of Symbols and Abbreviations

IoT	Internet of Things
IoMT	Internet of Medical Things
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
RFID	Radio-Frequency Identification
WPAN	Wireless Personal Area Network
WiFi	Wireless fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WSN	Wireless Sensor Networks
IAB	Internet Architecture Board

List of Tables

List of Figures

ACKNOWLEDGEMENTS

This dissertation would not have been possible without the help, support and patience of my principal supervisor, Prof. Sudhakar Ganti, not to mention his advice and unsurpassed knowledge of IoT, Fog Computing, Cloud computing and health informatics. The good advice, support and friendship of my committee member, Prof. Alex Kuo and Prof. Kui Wu, have been invaluable on both an academic and a personal level, for which I am extremely grateful.

I am profoundly grateful to my family (Man Wang, Bryan Guo and Nathan Guo) for their unwavering support, love, and encouragement throughout this journey. Their belief in me has been a constant source of strength and inspiration.

I would like to acknowledge the financial, academic, and technical support of the University of Victoria and its staff.

Chapter 1

Overview of IoT, Fog, and Cloud Computing in Healthcare

1.1 Introduction

Internet-of-Things (IoT) is an emerging technology that produces an ocean of data and applications. The Internet-of-Things (IoT) has become one of the most promising and rapidly developing technologies in recent years. IoT is a network of connected devices, machines, and sensors that are continuously communicating and exchanging data. The primary goal of IoT is to optimize our lives and drive economic advancement [1]. IoT has found its way into various fields, and healthcare is one such field where it has made a significant impact. In hospitals and homes, patients are increasingly interacting with various connected monitors, scanners, and sensors. These devices collect and transmit medical and life-related data to relevant healthcare providers and facilities, thereby helping to improve patient outcomes. The Internet-of-Medical-Things (IoMT) is a term used to describe the connected infrastructure of devices, software, hardware, and services that process and analyze health data for decision-making by healthcare professionals in patients' treatment. The rise of IoT in healthcare has led to exponential growth in the generation of medical records. Therefore, the need to improve the level of modern records management has become more pressing. Information technology, with its potential to tackle healthcare's three major challenges—rising costs, inconsistent quality, and limited access—has emerged as a promising solution. Cloud computing has become one of the most popular and promising information technologies. Cloud computing provides a secure and scalable platform for storing and processing medical data. This platform allows healthcare professionals to access medical records from anywhere in the world, which can lead to better diagnosis, treatment, and overall patient care. In conclusion, IoT and cloud computing are revolutionizing the healthcare industry, and it is an exciting time to be a part of this technological revolution. [2, 3].

With cloud computing emerging in recent years, more and more interest has been sparked from a variety of institutions, organizations, and individual users, as they intend to take advantage of web applications to share a huge amount of public and private data and information in a more affordable way and using reliable IT architecture. In the area of healthcare, medical and health information systems based on cloud computing are desired, to realize the sharing of medical data and health information, coordination of clinical service, along with effective and cost-contained clinical information system infrastructure via the implementation of a distributed and highly integrated platform. Cloud computing is one of the most prominent technological trends as it offers a platform for health information technology services over the Internet [4]. It is defined as an on-demand, self-service network architecture in which users can access computing resources and share information anytime from anywhere [5]. Cloud computing systems provide many benefits to facilitate medical information resource sharing. Within cloud computing, users or organizations gain the right to access medical records online, to engage their providers via digital channels, and to share their records across their teams of providers [6, 7, 8]. In addition, cloud computing reduces barriers to regulatory approval and licensing. Therefore, cloud computing accelerates the rapid sharing of clinical protocols, best practices and outcomes data without location restriction as best practice, standardized care procedures that can be supported. Cloud computing represents a "fourth space" beyond that healthcare has traditionally delivered: hospitals, clinics, and homes [9, 10]. Since health informatics seek new ways of driving healthcare information sharing forward, for example, international health information research collaboration are growing in demands, and now placed on computer networks to provide hardware and software resources and pave a new avenue to share sensitive and private medical data from different geographic locations. Cloud computing demonstrates tremendous opportunities for collaborative healthcare information sharing [11]. Users or the organization do not need to care about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes widely popular, thus missing potential customers and revenue. Although cloud computing has introduced a set of new and unfamiliar challenges [3, 6, 12], such as lack of interoperability, standardization, privacy, network security and culture resistance, it becomes a powerful tool to facilitate IoT devices and their data managements and manipulation given its unique features.

However, the pressure on IoT-Cloud systems has increased as more healthcare applications rely on real-time data collection and analysis to maintain the effectiveness and efficiency of IoT devices, such as heartbeat monitoring and life sensors. However, careful management of bandwidth is necessary to ensure that the IoT devices function properly. While cloud computing offers on-demand services and scalability, it may not be the most efficient way to process data for latency-sensitive IoT applications related to healthcare solutions with emergency response systems and content delivery applications, such as online monitoring systems, because the time required to transmit data to centralized servers and back can introduce delays that are unacceptable for critical real-time decision-making. The 2019 pandemic has highlighted the need for real-time public health monitoring data and timely big data analysis to prevent the spread of COVID-19. In the future, we will likely see the virus flare up at different times and in different places, requiring a rapid response to knock it back down. To prevent such outbreaks, a new transparent global public health monitoring system should be set up to probe disease outbreaks, empower healthcare systems and governments, and even the World Health Organization, to deploy investigators at short notice and reveal findings. This requires a robust and effective real-time monitoring and surveillance system with big data analytic capabilities. Fog computing offers advantages that meet the demands of healthcare applications requiring real-time, high response time, and low latency architecture. This technology provides a distributed computing infrastructure that enables data processing closer to IoT devices, reducing the latency and bandwidth requirements of cloud computing. With fog computing, data processing and analysis can be done in real-time, enabling quick responses to emergency situations. While cloud computing provides scalability and on-demand services, it may not be the most efficient way to process data for latency-sensitive IoT applications related to healthcare solutions. A new transparent global public health monitoring system is necessary to prevent future outbreaks, and fog computing provides a viable solution to meet the demands of healthcare applications requiring real-time, high response time, and low latency architecture.

The objective of this chapter is to present a comprehensive literature review on the integration of IoT, cloud computing, and fog computing to enable energy-efficient

Telehealth IoT systems, while also outlining the direction for my research. This review aims to identify the limitations of the current system and provide potential fog computing infrastructure solutions to improve resource sharing, system scalability, distributed processing, better security, fault tolerance, and privacy in healthcare application systems. An energy-saving model will meet the strict application requirements of IoT/fog/cloud systems without losing accessibility and flexibility, particularly in the healthcare area. To achieve these objectives, simulation studies will be conducted to demonstrate the effectiveness of the fog computing infrastructure in the healthcare application system. The case study will highlight how the integration of IoT, cloud computing, and fog computing can be used to monitor health data and facilitate real-time decision-making, improving the efficiency and effectiveness of healthcare services. The integration of IoT, cloud computing, and fog computing offers a promising solution for improving resource sharing, system scalability, distributed processing, better security, fault tolerance, and privacy of healthcare application systems. The energy-saving model and case study will provide practical examples of how this technology can be implemented to meet the strict application requirements of healthcare systems without sacrificing accessibility and flexibility.

Chapter 1 is organized as follows: We firstly introduced cloud computing with IoT, delineate its characteristic, service models, the combination of IoT with cloud computing, as well as issues and problems of applying cloud computing into IoT. The following section takes a close look at fog computing architecture, strength of fog computing compared with cloud computing, and how fog computing integrates with cloud computing and IoT. In the fourth section we examine analytics and big data in the context of IoT/fog/cloud computing infrastructure interest. The recognition that health care surveillance systems and applications demand real-time analytics as well as long-term global data mining illustrates the interplay and complementary roles of fog and cloud.

1.2 Overview of Cloud Computing and IoT Systems for Healthcare

1.2.1 Definition of Cloud Computing

Cloud computing has become a practical computing model that offers flexible, cost-efficient, and effective IT services to various types of users. The information technology realm requires constant and systematic innovation to provide high-quality services, and cloud computing has emerged as a leading solution to address this need. Cloud computing provides a platform for delivering IT services over the internet, enabling users to access computing resources and share information anytime and from anywhere. It offers a scalable and reliable infrastructure that can support the needs of businesses of all sizes, from small startups to large enterprises. With cloud computing, users can access a wide range of services, including storage, networking, computing, and security, without having to invest in expensive hardware and software. Cloud computing has become an essential tool for businesses looking to improve their efficiency and reduce costs. It offers a flexible and agile infrastructure that can adapt to the changing needs of businesses, allowing them to scale up or down as required. Additionally, cloud computing provides enhanced security, reliability, and data backup capabilities, ensuring that critical data is always accessible and protected.

Mell and Grance [5] give a definition of cloud computing that is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service-provider interaction. We have already seen similar more limited applications for years, such as Google Docs or Gmail. Nevertheless, cloud computing is different from traditional systems. Figure 1.1 shows the infrastructure of the NIST concept of cloud computing.

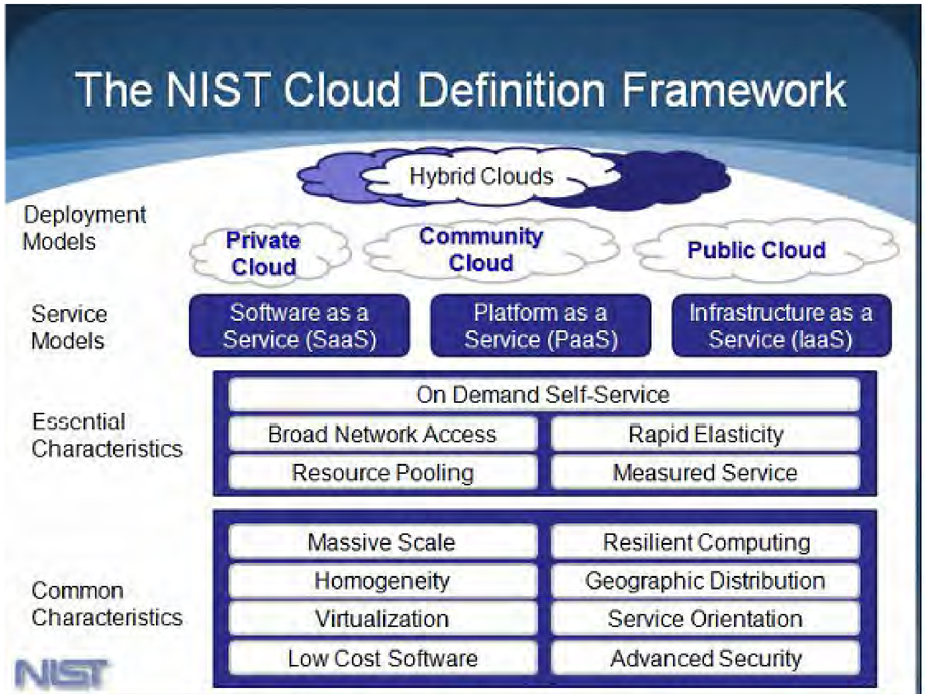

Figure 1.1: Cloud Computing Definition [12]

Armbrust et al. [12] state that cloud computing offers a wide range of computing sources on demand anywhere and anytime; eliminates an up-front commitment by cloud users; allows users to pay for use of computing resources on a short-term basis as needed and has higher utilization by multiplexing of workloads from various organizations. Cloud computing includes three models: (1) Software-as-a-Service (SaaS): the applications (e.g. EHRs) are hosted by a cloud service provider and made available to customers over a network, typically the Internet. (2) Platform-as-a-Service (PaaS): the development tools (such as OS system) are hosted in the cloud and accessed through a browser (e.g. Microsoft Azure). (3) Infrastructure-as-a-Service (IaaS): the cloud user outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The cloud service provider owns the equipment and is responsible for housing, running, and maintaining it. In the clinical environment, healthcare providers can remotely access the corporate Intranet via a local Internet service provider, since they can link with Cloud Computing system, as figure 1.2 shown [13].

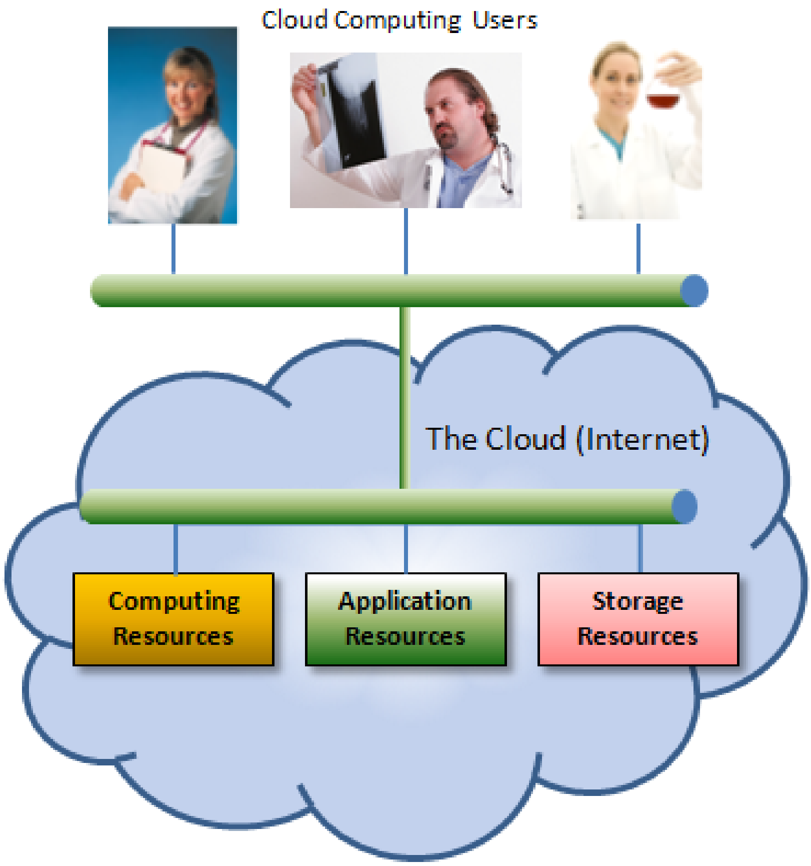

Figure 1.2: The Cloud Computing Platform [13]

A Cloud Computing service stack model is introduced by Guo et al [13]. The bottom two layers is a virtualization of resources in the form of storage and computing which is the foundation of cloud services. Virtual resource layer accesses lie on top of a cloud layer. It is an external application programming interface which provides the internal mechanism. Cloud service is not a separate service, but rather a collection of services. The model is shown in the figure 1.3 [13].

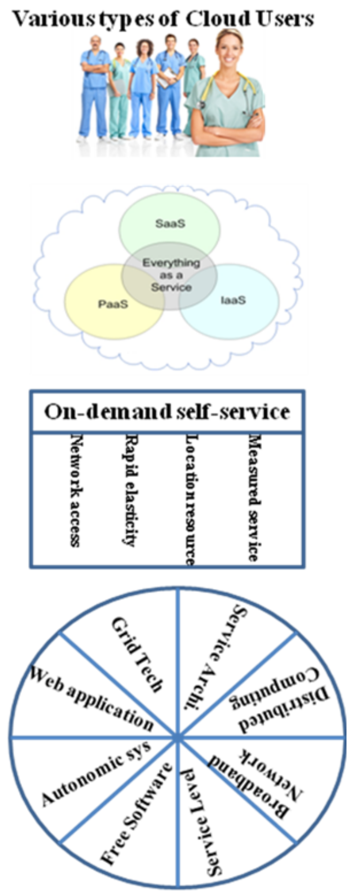

Figure 1.3: The Cloud Computing Service Stack Model [13]

1.2.2 Cloud Computing as Applied in Healthcare

Different types of organizations can benefit from cloud computing such as government agencies, financial enterprises, online entertainment companies, and healthcare providers. Cloud computing has been widely applied into the healthcare IT support areas. Currently, enhancing healthcare service quality and reducing the operational budget are the most important topics in the utilization of updated IT technologies in the healthcare area [14, 15, 16]. To achieve this goal, healthcare IT is highly intended to move departmental solutions to encompass larger strategy at the enterprise level, and from standalone systems that offer limited and localized solutions to more integrated and interconnected ones that bring up comprehensive and effective solutions [17]. Cloud computing has been deemed as an integrated solution that shifts the burden of managing and maintaining complex healthcare in-house high-cost hardware, software, and network infrastructure to the cloud, even the cloud service providers

[10, 11]. More specifically, healthcare information systems confront the high cost of implementing and maintaining IT, fragmentations of IT and insufficient exchange of patient data, lack of legal regulation mandating the use and protection of electronic health care data capture and communications, as well as lack of healthcare IT design and development standards [18, 19].

1.2.3 Definition of Internet-of-Things (IoT)

The Internet-of-Things is one of the modern paradigms of Information and Communication Technologies (ICT), which can bring advanced services for improving the quality of life of citizens and making better use of resources. IoT is commonly defined as the network of physical objects that are embedded with sensors, software and other technologies with other devices and systems over the internet. Namely, IoT is a robust network of things that is uniquely identifiable, where each of these objects connects to a datacenter that efficiently provides suitable services [20]. IoT enables us to communicate with each other and with the physical world by transferring pertinent data from the physical and virtual world. These things can give response to events around the world. All these processes can trigger activities and make events happen by human intervention or by machine-to-machine communication. Two driving factors to IoT are rapid increase of mobile devices and wide availability of wireless connectivity [21].

IoT has been widely used in ambient assisted living [22], smart cities [23] or smart logistics [24]. IoT is a rapidly growing trend in many areas, such as automotive, avionics, automation, energy, and health. The new sensing applications need enhanced computing capabilities to handle the requirement of complex and huge data processing which IoT could address by processing and communicating features to devices. IoT allows people and things to be connected anytime, anywhere with anything and anyone, ideally using any path/network and any service [25]. Although the current network infrastructure has provided capabilities and architecture for performing the computations and outsourcing the work from IoT devices, there is still much work to be done to properly accelerate our current IoT system to integrate with our computing resources. In short, the IoT integrates the interconnectedness of our society and culture with interconnectedness of our digital information internet system.

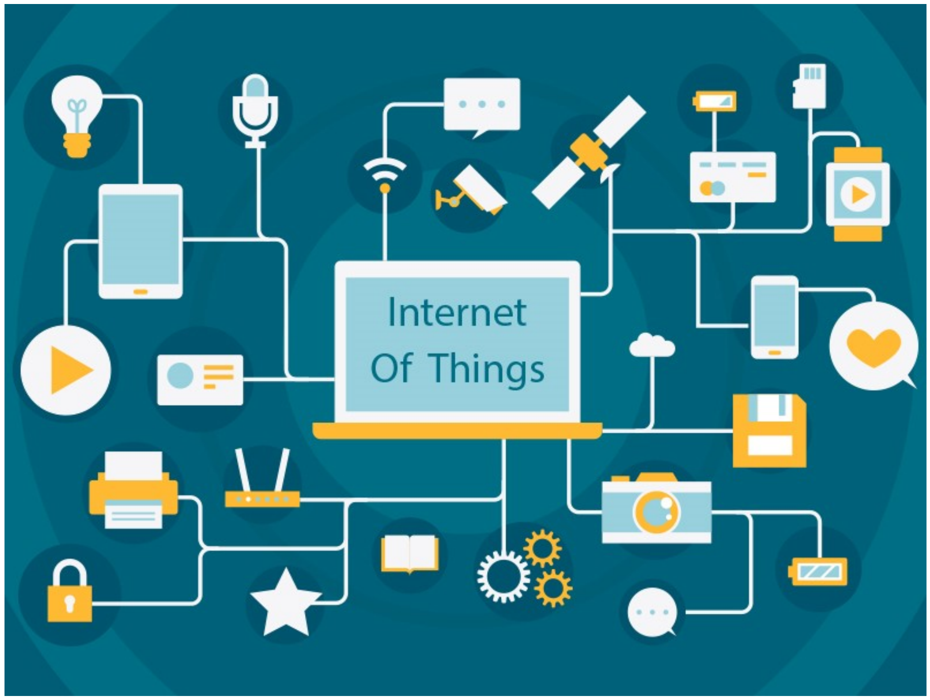

Figure 1.4: Internet-of-Things [25]

Initially, IoT was the most interesting to business and manufacturing, but as time progresses, more and more home and office applications are applied with smart devices, such that IoT is currently linked to with almost everyone. Recent applications have been developed with sensing and processing functions, and those devices usually have systems and mobile features such as smart phones, wearables, laptops, tablets, and so on. More recently, artificial intelligence served as a new technical advance starts to combine with IoT. This evolution enhances the digital transformation of society by offering people and experts with advanced applications for sensing and analyzing data on the ground [26]. As a result, IoT is expanding rapidly, as there are already more connected things than people in the world.

1.2.4 IoT Technologies

IoT technologies cover many unprecedented features, such as low price, small size and reducing energy consumption, and so on. Some technologies are briefly discussed below. Firstly, perception and identification of technology are the basis to support the long-term growth of IoT. Many IoT related technologies are listed as follows:

IoT related Technologies	Description
Radio-Frequency Identification (RFID)	Address short-range communication, which consists of a tag and a reader to communicate with each other for receiving and transmitting the signals.
Wireless Personal Area Network (WPAN)	One of the main parts in short-range IoT applications, which provides low-cost communication networks, consumes minimal power, and enables a reliable data transfer protocol [27].
Bluetooth	Another component of IoT technologies, and a type of wireless communication network developed for short distances. It can bring two or more devices and implement protection methods with encryption and authentication in a network.
ZigBee	A wireless technology to provide a foundation for IoT by enabling objects to work together, which includes end-nodes, routers, and a coordinator and processing center (data aggregation and data analysis) [28].
Wireless fidelity (Wi-Fi)	The principal component of IoT, and used in various fields, for instance, home automation, wearable sensor devices, mobile devices and smart grids [29].
Worldwide interoperability for Microwave Access (WiMAX)	It is executed in licensed and unlicensed frequency bands with transmit and receive antennas of the source and destination devices without a direct line of sight in between.
Mobile communication based on 2G, 3G and 4G	Widely used in our daily life, which is currently the predominant online communication network technologies, and it has been created as a global infrastructure to support different services effectively.

Continued on the next page...

IoT related Technologies	Description
Wireless Sensor Networks (WSN)	Comprised of heterogeneous sensors to detect and surveillance the living situations by applying three parts: nodes, routers, and a gateway to collect information from surroundings. WSN has many advantages to be used in IOT applications, for example, broad coverage, low installation cost and real-time data gathering [30].

Table 1.1: Descriptions of IoT related Technologies

1.2.5 IoT Architecture

The architecture of IoT has five layers, including business layer, application layer, middleware layer, network layer and perception layer, as shown in Figure 1.5 [31]. The business layer deals with the service and model work. It provides communication with clients for them to enhance their business service quality. Information is processed from the bottom layers and transferred back to it, thus earning better service quality from service providers. The application layer undergoes the final presentation of data which comes from the middle layer and offers global management of the application presenting that information. Given the requirements of users, the application layer can present the data in the form of smart city, smart home, smart hospital, vehicle tracking, smart farming, and many other kinds of applications. The middle layer receives data from the network layer. It enables service management and storage data. In addition, it can perform information processing and takes decisions automatically given the result and then give the outcome to the previous layer—application layer. Below the middle layer, it is a network layer, which is used to collect data from the bottom layer, like the network and transport layer of OSI model. After it collects data, the data can be sent to the internet. Sometimes, it also includes network management and information processing centers. The bottom layer is perception layer in the IoT architecture. As the name suggests, it is used to perceive the data from the upper layers and environment. All the data collected from the data sensing part is done on this layer, such as, sensors, bar code labels, RFID tags, GPS and camera. The main function of this layer is to identify objects and gather data.

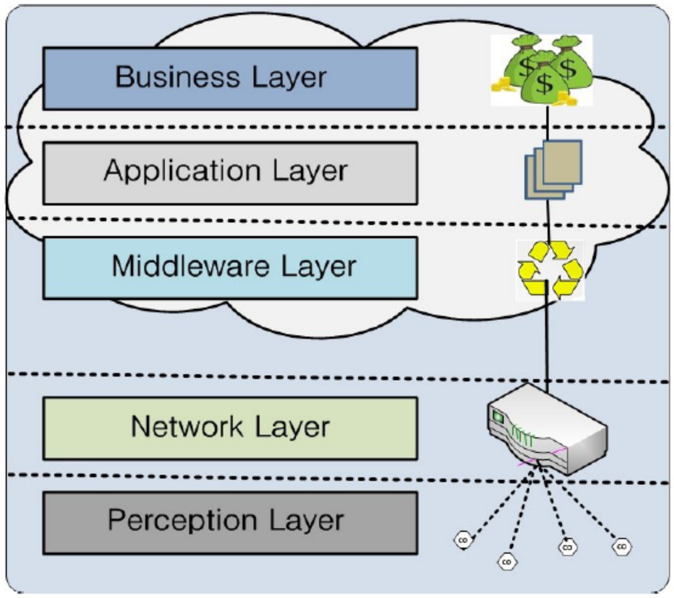

Figure 1.5: IoT architecture [31]

1.2.6 IoT Communication Models

The main objective of IoT is to connect different objects to the internet in different ways in which those objects can communicate with each other. Four types of communication modes are deployed according to the Internet Architecture Board (IAB) [31]:

A. Device-to-Device communication model: The communication model is based on IP networks to connect parties.

B. Device-to-Cloud communication model: IoT applications and devices are connected by the shortest route to the cloud service providers with TCP/IP network.

C. Device-to Gateway communication model: a communication software works as intermediary between IoT objects and the cloud. Most likely, smart devices, such as smartphone apps, perform the function of the gateway to exchange data between IoT devices and cloud servers. This model is fit for resolving interoperability issues with legacy systems.

D. Back-end Data-Sharing communication model: according to the security and confidential requirements, the sensitive data can be accessed by authorized users. The users are enabled to encrypt, aggregate, and export data from heterogeneous circumstances before sending the data to another user [31].

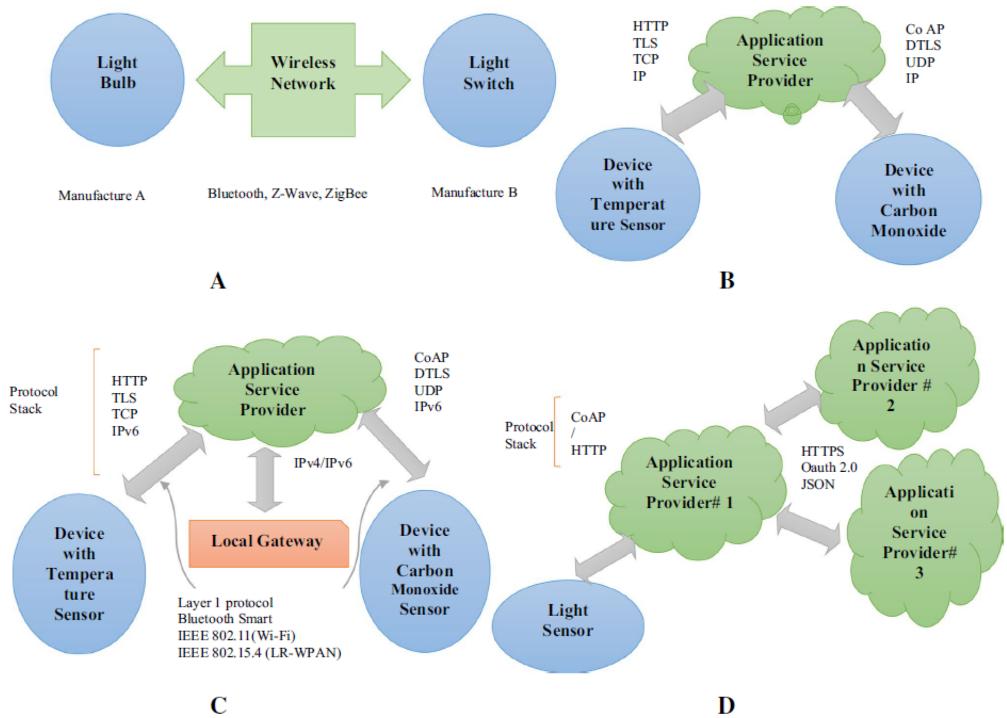

Figure 1.6: IoT communication models (a: Device-to-Device communication model, b: Device-to-Cloud communication model; c: Device-to-Gateway Model; d: Back-End Data-Sharing Model [31].

1.2.7 IoT Combined with Cloud

In the past few years, IoT devices have been integrated with cloud computing to increase the storage and data processing, as cloud service could provide a certain degree of scalability and interoperability, thereby making IoT devices more powerful and convenient to the end users at a low cost. For general use, the performance is improved because the communication between IoT sensors and data processing is faster. In addition, storage capacities, processing capabilities and cost can be significantly enhanced to some degree [32].

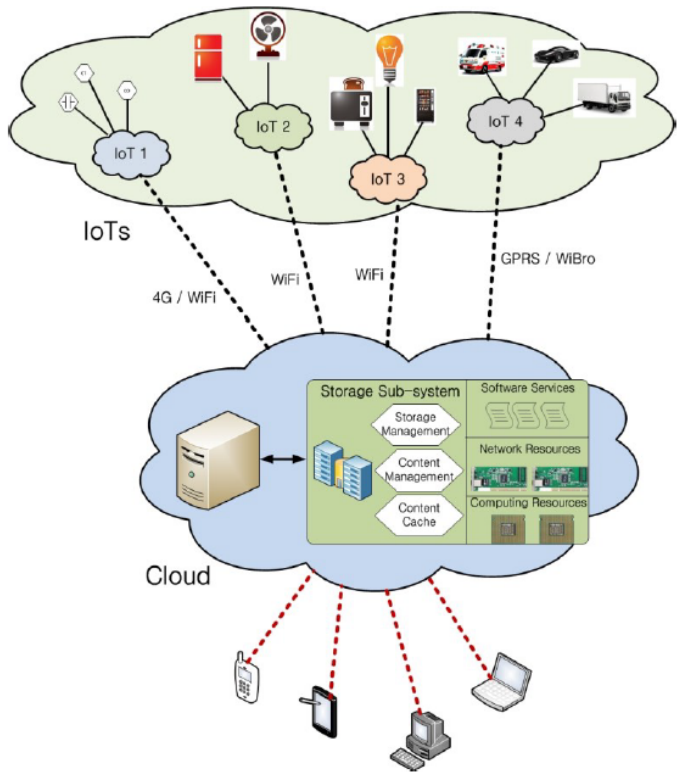

Figure 1.7: IoT devices connect with cloud [32]

1.2.8 IoT as Applied in Healthcare

With gradual special needs for aging population, shortage of healthcare human resources, and soaring healthcare expenditure, IoT-based technologies are playing a critical role in serving to address these challenges in healthcare. Recently, it has been seen that IoT devices and technologies are adopted in healthcare settings to a larger extent, due to faster service delivery, mitigating the increasing costs and improving service quality. As we know, IoT devices will empower patients to follow self-care principles, thus leading to cost-effectiveness of healthcare services, increased patient satisfaction and better self-management. More importantly, IoT technologies will enable the remote monitoring of physiological status in patients that used to consume huge amounts of healthcare providers' continuous attention [33, 34, 35]. Smart healthcare systems based on IoT devices and architecture have been developed. IoT has made revolutionary changes to the healthcare system, as it will offer more opportunities for patients to run tele-monitoring in hospitals and more importantly at home [36, 37]. Nowadays, patients are required to stay in the hospital for the whole duration of the treatment process, so the cost of our healthcare system is too high to endure. IoT devices offer the capability to remotely monitor patients given our current mobile network, thereby overcoming the challenge. IoT enables us to collect patients' real time health data and transfer them to healthcare providers, which not only saves the healthcare expenditure, but also provides the treatment before they become critical [38]. An IoT approach has been proposed to provide better health monitoring and control of weak health parameters, for instance, blood pressure, hemoglobin, blood sugar, etc., in which node location data and source transmit power for data are not mandatory. The results demonstrated that there was a substantial enhancement of the entire system with better energy consumption, latency, and throughput [39].

In general, IoT in the healthcare system can be categorized into three parts: homecare, mobile health, and hospital management. With respect to homecare, research indicates that most healthcare services will be transformed from hospital to homecare services by 2030 [40]. More healthcare functions will shift from hospital to home, such as vital signs monitoring, emergency management, telemedicine, and rehabilitation strategies in a stroke. Home healthcare based on IoT is a critical technology to tackle the healthcare dilemma associated with population aging. Home monitoring is among the outstanding applications of Wireless Sensor Networks (WSN), and we can use it to identify patients' activities [41]. In addition, sleep patterns can be detected and analyzed through IoT and is used for assessment of sleep quality in different ages and the evaluation of the medications effect for patients [42]. Secondly, mobile health with support of IoT technologies is ubiquitous recently, as the development of communication devices such as smartphones and their integration with different kinds of sensors. IoT promises to define both new approaches for patient and physician communications and better tailored therapeutic strategies to the patients. Moreover, immediate access to health data provides more chances to enhance the quality of clinical decisions and improve the patient's satisfaction and timely intervention. The maturity of IoT supported mobile health is linked to the internet to perform various telehealth services, for instance, tele-monitoring, supervision of seniors, tele-consultations and robotically assisted surgery [43, 44]. Finally, in hospital management, prevention of onsite infections, determination of patient education plan, management of emergency situations and logistics systems relate to IoT-based technologies, for example, sensors, RFID, NFC, etc. These technologies can overcome barriers in hospital logistic management and improve supply chain management by intelligently linking people, processes, and data to each other. Most recently, it has been recognized that vaccine supply needs to be enhanced by IoT innovation. Also, discharge care planning associated with IoT technologies is coming up gradually [45].

In summary, IoT applications have tremendous benefits:

- IoT-based healthcare technologies can be used for real-time monitoring from anywhere around the world to detect risky behavioral anomalies in patients.
- Locating and monitoring patients is enabled by IoT-based smart hospital management, so the hospital workflow and overall performance of patient care can be significantly improved.
- IoT can improve communication between different sections in hospital, thus leading to exchanging information and smart identification, tracking information more efficiently, finally it will be able to reduce healthcare costs and decrease hospital waiting and staying time of patients [46].

There is no doubt that low-cost healthcare services and their support, efficient surveillance of the centralized management system, as well as effective public health monitoring, can be attained with the fast development of IT-based technologies such as IoT and cloud computing. Nevertheless, due to its distributed, complex, and dynamic nature, IoT environment generates an ocean of data every moment from sensors, messaging system, mobile devices and social media, which are difficult to process in the cloud quickly. In addition, while healthcare always holds huge amounts of personal and patient information, we need to improve our understanding of the issues and opportunities of the IoT-based health care system. As we know, the design of IoT-based application and system is not straightforward as we thought, since we need to tackle simultaneous data interchange, data manipulation, processing complex mathematical function execution, which could overflow the computing capabilities of the embedded systems and mobile devices [47]. In addition, although IoT devices with wearable sensors provide attractive choices for enabling observation and recording, we still need to address many challenges in sensing, analyzing, and visualizing to fully integrating IoT into clinical practice.

1.3 Overview of Fog Computing Integration with IoT and Cloud Computing

As previously mentioned, revolutionary technologies such as IoT and cloud computing have been applied to the healthcare industry, creating unprecedented digital healthcare products, technologies, services, and opportunities. However, the integration of these technologies requires a combination of applications to meet the dynamic demands of the healthcare industry. These demands include cost-effective solutions that provide real-time support to patients, enabling early prediction and prevention of diseases and proactive treatment. Furthermore, public health systems require accurate and robust surveillance solutions to detect potential disease infection outbreaks, including new pandemics. However, the current IoT-cloud architecture is limited in its ability to meet these requirements due to significant delays in communicating data from IoT sensors to the cloud server. Moreover, cloud storage costs can be prohibitive, especially for large amounts of data. Therefore, fog computing has emerged as a potential solution to solve these issues in the healthcare system. Fog computing offers a distributed computing infrastructure that enables data processing closer to IoT devices, reducing the latency and bandwidth requirements of cloud computing. With fog computing, data processing and analysis can be done in real-time, enabling quick responses to emergency situations. This makes fog computing a promising technology for meeting the strict application requirements of healthcare systems, without sacrificing accessibility and flexibility.

1.3.1 Definition of Fog Computing

Fog computing, a term coined by Cisco, is an alternative to cloud computing that attempts to resolve two problems: the proliferation of computing devices and the opportunity presented by the data produced by these devices. By tackling certain resources and transactions at the edge of a network, fog computing provides a big advantage to users by avoiding bandwidth bottlenecks at access points and locating them closer to devices instead of establishing in-cloud channels for utilization and storage. This technology extends the traditional cloud computing to the edge of the network, bringing networking resources closer to the networks and serving as the middle part between IoT and cloud. Highly virtualized, fog computing provides computation, storage, and network services between IoT nodes and clouds, and targets services and applications with widely distributed deployments to improve the quality of service and better application.

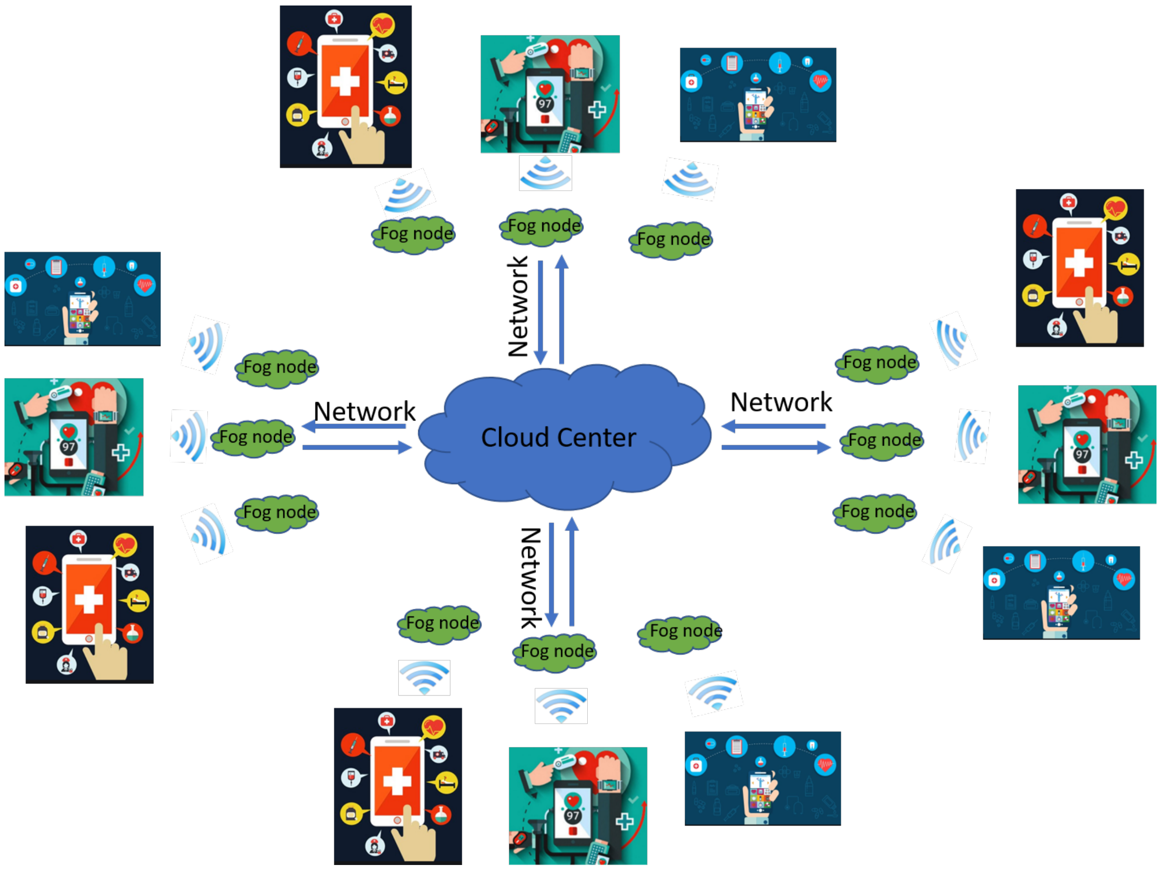

Figure 1.8: Fog Computing

Fog computing enables us to bring computing to the network's edge by moving storage and computing system as near as possible to the applications, components, and devices that need them. Also, processing latency is removed or greatly reduced. These characteristics are needed for IoT connected devices, which could generate huge amounts of data and require rapid processing [48].

The differences between cloud and fog computing are addressed in the table below [48]:

Feature	**Cloud Computing**	**Fog Computing**
Architecture	Centralized	Distributed
Communication with devices	From a distance	Directly from the edge

Feature	Cloud Computing	Fog Computing
Data processing	Far from the source of information	Close to the source of information
Computing Capabilities	Higher	Lower
Number of nodes	Few	Very large
Analysis	Long-time	Short time
Latency	High	Low
Connectivity	Internet	Various protocols and standards
Security	Lower	Higher
Big data storage	Short duration and targeted to specific area	Lifetime duration as it manages big data
Working environment	Streets, roadside, home, and malls	Indoors with massive components at cloud service provider-owned place
Number of users facilitated	Locally related fields	General internet-connected users
Location identification	Yes	No
Mobility features	Provided and fully supported	Limited
Major service providers	Google, Amazon, IBM	Cisco IOx, Intel

Table 1.2: Cloud and fog computing comparison [48]

1.3.2 Fog Computing Architecture

According to Figure 1.9 [49], the architecture of fog computing consists of three layers: the Cloud Layer, the Fog Layer, and the IoT Device Layer. The Cloud Layer serves as a data center capable of storing vast amounts of data with minimal response time. The Fog Layer, situated in the middle, contains numerous fog nodes used for big data analysis and aggregation. The bottom layer, the IoT Device Layer, is responsible for generating data through sensing and processing. A variety of devices are connected at the network's terminal to enable adaptable communication, storage services, collaborative computing, and variable functionalities.

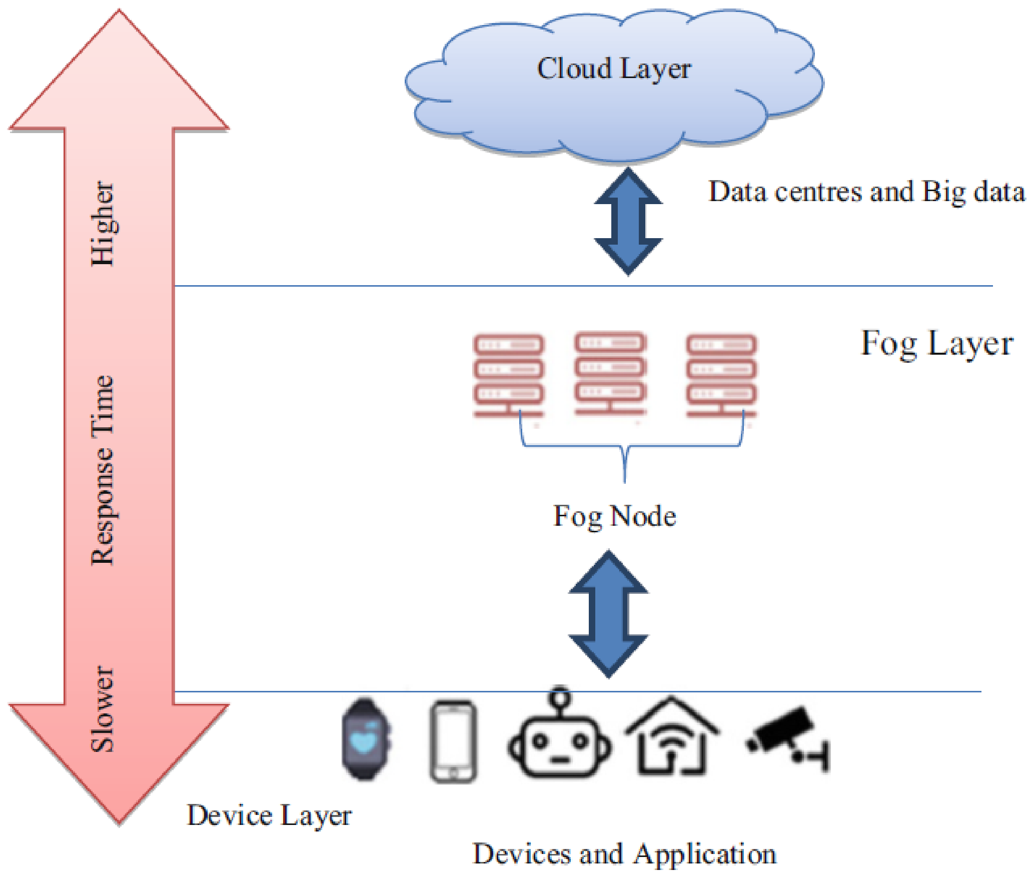

Figure 1.9: Architecture of Fog Computing [49]

Compared to the traditional cloud/IoT framework, fog computing architecture offers several advantages, such as real-time processing, low latency, and high responsiveness. Positioned between the cloud and IoT devices, fog computing ensures geographically distributed nodes that provide enhanced computational power, greater storage capacity, and improved network connectivity.

In the healthcare sector, fog computing architecture addresses critical health IT challenges. For instance, when patients consult healthcare providers through IoT devices, rapid data analysis and diagnosis are essential for timely and effective treatment. Fog computing can mitigate healthcare challenges caused by time constraints or insufficient resources, enabling faster response times and more efficient resource utilization.

1.3.3 Pros and Cons of Fog Computing

The benefits of fog computing are obvious compared with cloud computing and current other technologies. The following are the main advantages of fog computing:

- Low latency: it is geographically closer to users so it can provide instant responses.
- Avoiding bandwidth bottleneck: collecting information and data happens at many edge points instead of sending them together to one data center via the internet.
- High availability: it has multiple interconnected channels.
- High security: data in fog computing is processed in different nodes in a complex distributed system.
- Better user experience: it satisfies the need for rapid response and no downtimes.
- Power efficiency: edge nodes run power-efficient protocols.
- High usability: it is possible for a fog system to be installed on low specification devices like switches and IP cameras.
- High flexibility: fog computing has relatively small computing resources (memory, processing, and storage) compared with cloud computing, but the resources can be enhanced if needed.

Technically, the cons of fog computing are not significant compared with our existing technologies, but a few shortcomings could be listed as follows:

- More complicated system: increasing one more layer in the system can increase the complexity for system maintenance and upgrade.
- Additional expense: a new layer is added which costs more for extra devices, such as routers, hubs, and gateways.
- Limited scalability: fog has limited scalability in comparison to cloud.

1.3.4 Fog Computing as Applied in the Healthcare

With more and more IoT devices involved in the healthcare area (skin sensors, heart rate sensor, wearable sensor, chemical sensor, glucose sensor, etc), the characteristic of the system is being changed as follows [50, 51]:

- Mobilized data.
- Geographically distributed and decentralized.
- Heterogeneous
- Security and privacy are concerned with severe disease.
- Real-time, rapid, accurate analysis and safe clinical decision
- Continuous and timely observations for critical patients
- Minimize repetition of investigative testing, imaging, and past records.
- Efficient and effective medication
- Increased fast implementation of testing and examining requirements and protective health procedures.

Because of network bandwidth restrictions, cloud computing alone cannot provide small enough latency time for processing the data and transfer them back to the healthcare providers, thus decreasing the use of health data and operation efficiently. Given these new features, healthcare IT became a uniquely challenged area that fog computing architecture could address with its remarkable advantages [52]:

- Low latency time
- Real time rapid interaction
- Process the data in a fast time manner such that data is available to all stakeholders.
- Interoperability and scalability
- Location awareness for the decentralized and distributed data
- Seamless security and privacy constrain mechanism

1.4 Requirements of Integrating IoT/Fog/Cloud Computing System

As we know, IoT requires a substantial amount of computer and storage resources, especially when it is applied to the healthcare industry. The design and requirements of IoT applications with cloud and fog computing need to create a general and multipurpose platform that can serve a wide variety of IoT applications. This platform allows IoT to offload some computation tasks onto other areas quickly and with minimum energy consumption. As a result, an adaptable and scalable IoT/fog/cloud platform is necessary to meet the demands of IoT applications in various industries, including healthcare.

- The system for IoT/Fog/cloud must support rapid mobility patterns, even requiring in some cases high throughput on demand for short time periods.
- The system must support an integrated system requiring reliable sensing, analysis, control and actuation, in scenarios subject to poor or unreliable connectivity to the cloud and or requiring very low latency.
- The platform for IoT/fog/cloud is required to able to manage a large amount of geographically distributed "things", either physically or virtually, which may produce data that require different levels of real-time analytics and data aggregation.
- The platform must have add-in security measures and adopt a security-centric to protect the distributing system, thereby determining the possible security gaps, analyzing existing security solutions and then putting forwards a list of comprehensive security solutions that can eliminate many potential securities of flaws.

1.5 Summary

The integration of IoT, fog, and cloud computing architectures holds immense potential to enhance the quality of healthcare services by improving scalability and mobility while significantly reducing energy consumption across the three layers during data processing and transmission. To realize these objectives, this research demonstrates a hybrid model that serves as an advanced resource management framework, offering numerous benefits in terms of efficiency and effectiveness.

The model and algorithms will be thoroughly evaluated through comprehensive research, contributing valuable insights to the existing body of knowledge on IoT, fog, and cloud computing integration, particularly in the context of telehealth. This research aims to advance resource management practices and promote more energy-efficient healthcare solutions.

Finally, we expect this work to meet institutional expectations and make meaningful contributions to the research community. The rest of the dissertation is organized as follows: Chapter 2: Energy-Efficient Telehealth IoT Systems: Integrating Fog and Cloud Computing for Sustainable Data Processing. Chapter 3: Enhancing Energy Efficiency in Telehealth IoT through Multi-Objective Optimization on a Hybrid Fog/Cloud Computing Platform. Chapter 4: Conclusion and Future Directions These chapters detail the research results and innovations that address critical challenges in telehealth systems and pave the way for sustainable, energy-efficient healthcare IT infrastructures.

Chapter 2

Energy-Efficient Telehealth IoT Systems: Integrating Fog and Cloud Computing for Sustainable Data Processing

2.1 Introduction

Healthcare is a critical global industry, and the advent of the Internet-of-Things (IoT) and cloud computing has significantly transformed healthcare system management. The ever-increasing data volume generated by these systems demands efficient, energy-saving computing platforms. In response, we present a ground-breaking energy-efficient model that seamlessly integrates telehealth IoT devices with fog and cloud computing-based platforms, offering a unique solution to address energy efficiency and data processing challenges.

The rapid proliferation of IoT devices in healthcare has transformed approaches to patient care, diagnostics, and treatment. Telehealth, a key IoT healthcare application, has proven its potential to enhance care quality, reduce costs, and boost patient satisfaction. Despite these benefits, issues such as scalability, latency, and resource management persist, along with the significant challenge of energy consumption in smart devices within fog environments [53]. As a result, energy efficiency must be prioritized in the development of fog computing solutions, given its substantial impact on reducing carbon footprints and mitigating climate change effects. The large-scale deployment of telehealth IoT devices also raises concerns about energy consumption and data processing efficiency in delivering quality healthcare services. Intelligent choices for telehealth IoT devices should consider factors such as device movement or relevant environmental conditions to optimize energy consumption and manage associated equipment new parameters. Typically, cloud-based analytical assessments are conducted for these devices [54]. To tackle these challenges, we propose an energy-saving model that integrates telehealth IoT devices with a fog and public/private cloud computing-based platform to optimize data processing without compromising real-time healthcare services. By incorporating fog computing as an intermediary layer between IoT devices and public or private cloud servers, the model enables localized data processing, effectively reducing latency and data transfer overhead. Simultaneously, public and private cloud computing provides a robust infrastructure for handling large data volumes and performing resource-intensive computations.

The primary goal of this model is to minimize energy consumption through intelligent task allocation between fog nodes and cloud servers, by considering their computational capacity and proximity to IoT devices. This task allocation process also considers various sensitivity and priority levels within the healthcare context, ensuring prompt responses to critical and high-sensitivity requests. Our model synergistically combines the strengths of fog and cloud computing, creating an energy-efficient telehealth IoT system that effectively manages data processing and delivers real-time healthcare services in accordance with various levels of sensitivity and priorities. Moreover, a simulation method is employed to evaluate the effectiveness and efficiency of the system, as examining complex IoT-Fog-Cloud systems within a simulation environment is a prevalent approach among researchers. This is because exploring diverse large-scale network topologies, involving thousands of IoT devices, is rarely feasible in the real world. Although the requirements for such a simulator are straightforward—providing a detailed, accurate, and granular model of all components—implementing corresponding simulators demands considerable effort.

2.2 Overview of Telehealth IoT Devices

2.2.1 Definition of IoT Devices

Telehealth IoT devices refer to a wide range of interconnected medical devices and sensors that facilitate remote healthcare services. These devices enable the continuous monitoring of patients' vital signs, timely diagnostics, and personalized treatment plans, thereby improving the overall quality of healthcare. Some common examples of telehealth IoT devices include wearable health monitors, smart glucose meters, remote patient monitoring systems, and telemedicine platforms.

2.2.2 Challenges of Large-Scale Deployment

The large-scale deployment of telehealth IoT devices presents several challenges, including [55]:

1. Energy Consumption: Telehealth IoT devices require a continuous power supply to operate and communicate with other devices and servers. As the number of devices increases, so does the overall energy consumption. This poses a challenge in terms of energy efficiency, especially for battery-powered devices, and raises concerns about the environmental impact of such deployments.

2. Data Management: The vast amount of data generated by telehealth IoT devices demands efficient data management solutions. Storing, processing, and analyzing this data in real-time can be resource-intensive, putting a strain on both network and computing infrastructures.

3. Latency: Real-time healthcare services require low-latency communication between IoT devices and servers. However, as the number of devices increases, network congestion and longer transmission distances can result in higher latency, affecting the quality of healthcare services.

4. Security and Privacy: Protecting sensitive patient data and ensuring the privacy of healthcare information are critical concerns in telehealth IoT deployments. The large-scale implementation of such devices exposes them to potential cyberattacks and data breaches, requiring robust security measures and encryption techniques.

5. Scalability: The rapid growth of telehealth IoT devices necessitates scalable solutions that can accommodate an increasing number of devices without compromising performance, reliability, or efficiency.

6. Interoperability: Telehealth IoT devices often need to communicate with a variety of other devices and platforms. Ensuring seamless interoperability between

different devices and systems is a challenge that must be addressed to provide effective and integrated healthcare services.

In the following section, we will review the fundamentals of fog and cloud computing and explore how they can be leveraged to address these challenges in large-scale telehealth IoT deployments.

2.3 Fundamentals of Fog and Cloud Computing for Large-Scale Telehealth Deployment

2.3.1 Fog Computing

Fog computing, also known as edge computing, is a distributed computing paradigm that brings computation, storage, and networking resources closer to the data sources, typically IoT devices. By performing data processing and analytics at the edge of the network, fog computing can effectively address the challenges of latency, network congestion, and energy consumption.

Key advantages of fog computing in telehealth IoT deployments include:

1. Reduced Latency: By processing data locally, fog computing can significantly reduce the time taken for data to travel between IoT devices and cloud servers, ensuring low-latency communication and real-time healthcare services.

2. Energy Efficiency: Local data processing reduces the amount of data transmitted over the network, resulting in lower energy consumption for data transmission and device operation, because local data processing can reduce the amount of data transmitted over the network, minimize network congestion, decrease latency, lessen the reliance on centralized infrastructure, shorten transmission distances, and enabling adaptive data processing, all of which contribute to lower energy consumption for data transmission and device operation.

3. Enhanced Privacy and Security: Fog computing enables data processing at the edge, which minimizes the need to transmit sensitive patient data over the network, reducing exposure to potential security risks and data breaches.

2.3.2 Cloud Computing

Cloud computing is a computing paradigm that offers on-demand access to a shared pool of computing resources, such as servers, storage, and applications, over the internet. Cloud computing provides the infrastructure required for large-scale data storage, processing, and analytics, making it an ideal solution for managing the vast amounts of data generated by telehealth IoT devices.

Key advantages of cloud computing in telehealth IoT deployments include:

1. Scalability: Cloud computing offers virtually unlimited resources, making it easy to scale up or down as the number of telehealth IoT devices and data volume increase.

2. Cost-Effectiveness: Cloud computing allows healthcare providers to access powerful computing resources without the need for large upfront investments in hardware and infrastructure, enabling a pay-as-you-go model that can be more cost-effective.

3. Advanced Data Analytics: Cloud platforms often provide advanced data analytics tools and machine learning capabilities that can be leveraged to derive valuable insights from the collected healthcare data, improving diagnostics and treatment plans.

2.3.3 Leveraging Fog and Cloud Computing to Address Telehealth IoT Challenges

Integrating fog and cloud computing in telehealth IoT deployments can harness the benefits of both paradigms, creating a synergistic solution that addresses the challenges:

1. Energy Efficiency: By intelligently allocating tasks between fog nodes and cloud servers based on proximity and computational capacity, energy consumption can be optimized.

2. Latency Reduction: Fog computing ensures low-latency communication for real-time healthcare services, while cloud computing provides the resources for large-scale data processing and analytics.

3. Enhanced Security and Privacy: Fog computing enables local data processing, reducing the need to transmit sensitive data, while cloud platforms provide robust security measures to protect stored data.

4. Scalability and Interoperability: The combination of fog and cloud computing offers a scalable solution that can accommodate a growing number of telehealth IoT devices, while ensuring seamless communication between various devices and platforms.

In the next section, we will introduce the energy-saving model that integrates telehealth IoT devices with a fog and cloud computing-based platform.

2.4 Related Work

In this section, we will review the existing literature on telehealth IoT devices, fog computing, cloud computing, and energy-saving models, providing the background and motivation for the development of the energy-saving model.

2.4.1 Telehealth IoT Devices

Telehealth has emerged as a promising solution to address various challenges in healthcare, such as accessibility, cost, and quality of care [56]. IoT devices play a significant role in telehealth applications, enabling remote monitoring, diagnostics, and treatment [54]. Several studies have investigated the implementation and efficacy of telehealth IoT devices in various healthcare scenarios, highlighting their potential to improve patient outcomes and satisfaction [57, 58].

2.4.2 Fog Computing in Healthcare

Fog computing has been identified as a promising approach to address the challenges associated with large-scale IoT deployments in healthcare, such as latency, energy consumption, and data management [59, 60]. Researchers have proposed several fog computing-based architectures and frameworks for healthcare applications, demonstrating the potential of fog computing to enhance the performance and efficiency of telehealth IoT devices [61, 62, 63].

2.4.3 Cloud Computing in Healthcare

Cloud computing has gained significant attention in healthcare due to its scalability, cost-effectiveness, and advanced data analytics capabilities [64, 65]. Several studies have explored the integration of cloud computing with telehealth IoT devices, showing its potential to address the challenges related to data storage, processing, and security [66, 67, 51].

2.4.4 Energy-saving Models for IoT Devices

Energy efficiency is critical in large-scale IoT deployments, especially in healthcare applications where longevity and reliability are essential [68]. Researchers have proposed various energy-saving models and strategies for IoT devices, including adaptive power management [69], energy-efficient routing protocols [70], and data compression techniques [71]. However, few studies have specifically focused on energy-saving models that integrate telehealth IoT devices with fog and cloud computing-based platforms.

2.4.5 Fog and Cloud Computing Integration

The integration of fog and cloud computing has emerged as a promising approach to harness the benefits of both paradigms and address the challenges of large-scale IoT deployments [72, 73]. Several studies have proposed models and frameworks that combine fog and cloud computing for various IoT applications [74, 75, 76], but few have specifically targeted energy-saving in telehealth IoT deployments.

2.4.6 Simulation Methods in the Context of Fog Computing, IoT Devices, and Cloud Computing

In recent years, several simulation methods have been developed to study the integration of fog nodes in IoT devices and cloud computing. Gupta [77] introduced iFogSim, a toolkit for modeling and simulating resource management techniques in IoT, edge, and fog computing environments. Oueis [78] presented a simulation study on load distribution in small cell cloud computing using fog computing and proposed a fog balancing technique to optimize resource allocation and reduce latency. Barcelo [79] explored IoT-cloud service optimization through simulation in smart environments, presenting a novel optimization framework that utilizes fog nodes to reduce latency and energy consumption. Zeng [80] conducted a comparative study of IoT cloud and fog computing simulations using iFogSim and Cooja, discussing the advantages and limitations of both simulators and providing insights into selecting an appropriate tool for specific scenarios. Lastly, Byers and Wetterwald [81] discussed the concept of fog computing and its importance in distributing data and intelligence for IoT resiliency and scalability, presenting various simulation models and techniques used to evaluate the performance of fog computing in IoT environments. Several studies have focused on the YAFS (Yet Another Fog Simulator) framework, a simulator designed for modeling and simulating fog computing environments in IoT scenarios. Bermejo [82] introduced YAFS, presenting the architecture, components, and use cases of the simulator, demonstrating its effectiveness in modeling and simulating fog computing deployments. García [83] showcased YAFS's ability to model and simulate fog computing scenarios and analyze the performance of different scheduling algorithms. In a comparative study, Guo et al. [84] analyzed the features, capabilities, and limitations of YAFS, iFogSim, and EdgeCloudSim simulators, providing insights into selecting the most suitable tool for specific fog computing scenarios.

2.4.7 Simulation Methods to Study IoT Device Energy Saving Model in the Fog and Cloud Nodes in Healthcare

Several studies have explored different aspects of telehealth simulations, fog nodes, IoT devices, and cloud computing for energy-saving purposes. Aazam and Huh [85] discussed a smart gateway-based communication approach using fog computing for energy-saving in the Cloud of Things, which can be applied to various IoT applications, including telehealth. Verma and Sood [86] presented a fog-assisted IoT framework for patient health monitoring in smart homes, focusing on energy efficiency and reduced latency through a decentralized fog computing architecture. Koubaâ [87] proposed a fog-based emergency and healthcare system for smart cities, leveraging fog nodes and IoT devices to optimize energy consumption and provide real-time healthcare services, addressing energy-saving concerns in telehealth scenarios. Sareen [88] introduced an energy-efficient context-aware framework for managing application execution in cloud-fog environments, which can potentially improve energy efficiency in various IoT applications, including telehealth scenarios.

This literature review highlights the potential of fog and cloud computing in addressing the challenges of large-scale telehealth IoT deployments, as well as the need for energy-saving models that integrate both paradigms. In response to this gap in the literature, the dissertation utilizes an energy-saving model that combines fog and cloud computing to optimize energy consumption in telehealth IoT devices according to different levels of sensitivities and priorities while ensuring efficient data processing and high-quality healthcare services.

2.5 Energy-Saving Model for Telehealth IoT Devices with Fog and Cloud Computing-Based Platform

2.5.1 Model Overview

The energy-saving model is designed to integrate telehealth IoT devices with a fog and cloud computing-based platform, leveraging the advantages of both paradigms to optimize energy consumption and ensure efficient data processing. The model comprises three main components: IoT devices, fog nodes, and public/private cloud servers, interconnected through a communication network.

2.5.2 Model Architecture

1. IoT Devices: Telehealth IoT devices, such as wearables, sensors, and remote monitoring systems, collect and transmit patient data in real-time. These devices can dynamically adjust their power states (e.g., active, idle, sleep) based on their tasks, reducing energy consumption without compromising the quality of healthcare services.

2. Fog Nodes: Fog nodes, located near IoT devices, serve as intermediate processing units. They perform localized data processing, analytics, and storage, reducing the amount of data transmitted to the cloud servers. Fog nodes can also dynamically adjust their power states to optimize energy consumption.

3. Cloud Servers: Cloud servers provide a robust infrastructure for large-scale data storage, processing, and advanced analytics. They manage resource-intensive tasks and coordinate with fog nodes to balance the workload, ensuring efficient data processing and energy usage.

4. Communication Network: A communication network connects IoT devices, fog nodes, and cloud servers, enabling seamless data transmission and task allocation. The network must be designed to minimize latency and energy consumption while maintaining secure and reliable communication.

The model architecture is shown in Figure 2.1 [89] below:

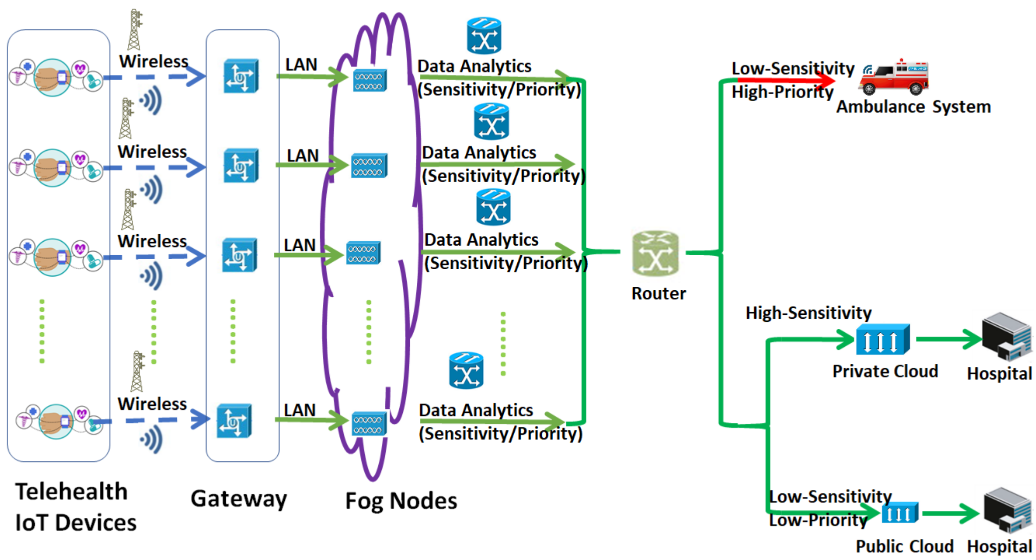

Figure 2.1: Telehealth IoT devices integrated with Fog nodes and private/public cloud architecture model

The telehealth IoT network depicted in the diagram is designed to ensure efficient and secure data transmission between the different network components. To ensure network security, firewalls are placed between IoT devices and fog nodes. This ensures that unauthorized access to the network is prevented, and sensitive healthcare data is kept confidential.

To process the data requests, the fog nodes are equipped with data analytics functions that enable them to intelligently assign different types of requests to either fog nodes, private cloud, or public cloud. This intelligent decision-making process is more effective and efficient than the traditional "first-come, first-served" approach.

The gateway and router are integral components in the network that enable seamless data transmission between fog nodes and cloud instances. The gateway acts as the entry point for the network and connects the IoT devices to the local fog nodes. It is responsible for handling the data transmission and conversion between different protocols used by IoT devices and fog nodes.

The router, on the other hand, is responsible for directing the data traffic between the fog nodes and cloud instances based on various factors, such as the sensitivity, priority, and latency requirements of the data. It determines which data should be sent to the cloud and which data should be processed by fog nodes, ensuring efficient use of network resources. The router also handles communication between different fog nodes and cloud instances, enabling seamless data transmission across the network.

The network topology is shown below (Figure 2.2)

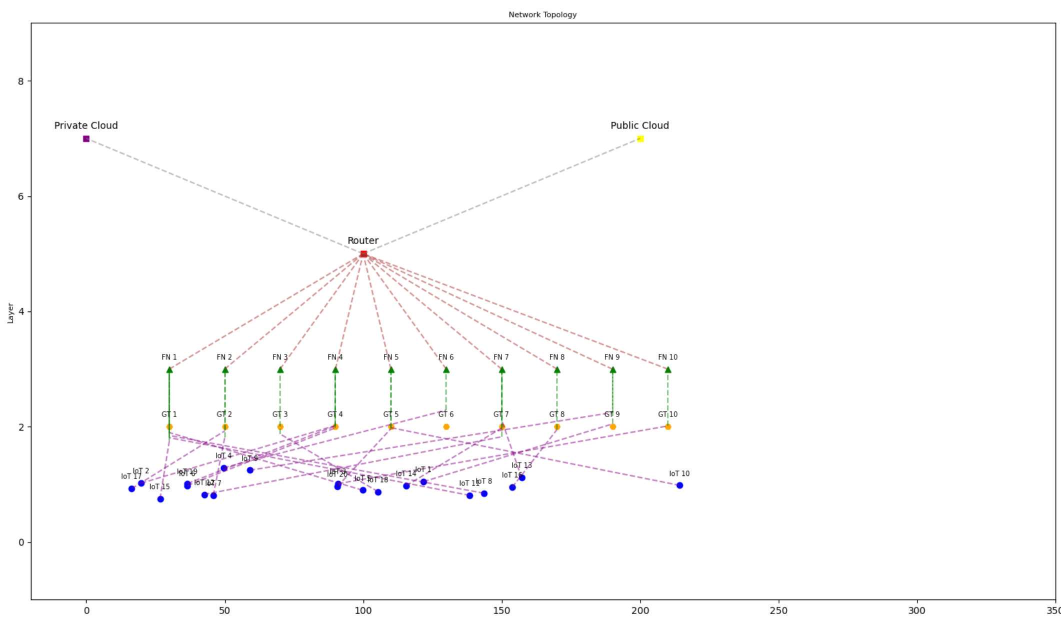

Figure 2.2: Network Topology for the IoT devices integrated with Fog nodes and Cloud.

Here is a brief overview of the components in the network topology:

- IoT devices (blue circles) represent individual IoT devices in the network, each associated with a specific fog node.
- Gateways (orange hexagons) are used to connect the IoT devices to the fog nodes.
- Fog nodes (green triangles) are intermediate computing resources that process and store data from IoT devices.

- A router (red square) connects the fog nodes to the private cloud and public cloud.

- Private Cloud (purple square) and Public Cloud (yellow square) are the two cloud resources in the network.

The telehealth IoT system intelligently manages data transmission based on the sensitivity and priority of the data. For high-sensitivity data, the system ensures privacy and security by sending it directly to the private cloud, which then transfers the data to authorized health facilities as needed. On the other hand, low-sensitivity but high-priority requests are routed to fog nodes as they have the capability to process urgent requests in a timely manner, such as in life-threatening emergency situations. These requests are then transmitted to ambulance systems for immediate treatment. Lastly, data with low sensitivity and low priority are sent to the public cloud as it has more space and scalability to store and process such data. The public cloud can also serve as a repository for future research or clinical purposes.

By allocating data transmission to the appropriate destination, the system ensures efficient and effective data processing, while maintaining privacy and security for sensitive healthcare data. This approach also optimizes energy consumption and reduces latency, ensuring a seamless experience for healthcare providers and patients.

The categorization of high and low sensitivity and high and low priority data sent from telehealth IoT monitor devices can depend on various factors, including the specific use case, regulatory requirements, and patient needs. One possible approach could be to use threshold values based on vital signs such as pulse and heartbeat to categorize the data.

For example, data related to vital signs that fall within normal ranges may be classified as low sensitivity and low priority, as they do not require immediate attention. Data related to vital signs that are outside the normal range but do not pose an immediate threat to the patient's health may be classified as low sensitivity but high priority. Data related to vital signs that indicate a life-threatening condition, such as cardiac arrest, may be classified as high sensitivity and high priority, requiring immediate attention from healthcare providers.

The exact vital sign thresholds for patient emergencies can vary depending on a range of factors, including the age and health condition of the patient, the specific symptoms, and another medical history [90]. In general, some common vital sign thresholds used to classify emergencies include:

- Heart rate: A heart rate above 100 beats per minute (BPM) or below 60 BPM may be indicative of an emergency. [91]
- Blood pressure: A systolic blood pressure (the top number) above 180 mm Hg or below 90 mm Hg, or a diastolic blood pressure (the bottom number) above 110 mm Hg or below 60 mm Hg may indicate an emergency. [92]
- Respiratory rate: A respiratory rate above 30 breaths per minute or below 10 breaths per minute may be indicative of an emergency. [93]
- Oxygen saturation: An oxygen saturation level below 90% may be indicative of an emergency. [94]

However, it is important to note that this is just one possible approach, and the categorization of data should be customized based on the specific needs of the patient and healthcare provider. It is also important to comply with relevant regulations and ensure patient privacy and security while handling sensitive healthcare data.

2.5.3 Key Components and Energy-Saving Strategies

The energy-saving model incorporates several strategies to minimize energy consumption:

1. Task Allocation: The model intelligently allocates tasks between fog nodes and cloud servers based on factors such as computational capacity, proximity to IoT devices, and current workload. This ensures efficient data processing and reduces energy consumption for data transmission.
2. Adaptive Power Management: IoT devices and fog nodes can dynamically adjust their power states (e.g., active, idle, sleep) based on their tasks and workload, ensuring optimal energy consumption without compromising the quality of healthcare services.
3. Data Compression and Aggregation: Data generated by IoT devices can be compressed and aggregated at the fog nodes before transmission to cloud servers, reducing the volume of data transmitted and, consequently, energy consumption.

4. Network Optimization: The communication network can be optimized to minimize energy consumption by employing energy-efficient routing protocols and minimizing transmission distances.

In the next section, we will present a simulation study to evaluate the effectiveness of the energy-saving model in real-world telehealth scenarios.

2.6 Simulation Study: Evaluating the Effectiveness of the Energy-Efficient Model

2.6.1 Simulation Analysis

To assess the effectiveness of the energy-efficient model, we developed a simulation model that emulates a real-world telehealth scenario focused on remote patient monitoring. Within this simulated scenario, numerous patients with chronic conditions are equipped with wearable IoT devices that continuously track vital signs such as heart rate, blood pressure, blood glucose levels, etc. The gathered data is processed and analyzed by the integrated fog and cloud computing-based platform, facilitating timely diagnostics and personalized treatment plans.

Here is the pseudo-code of the model:

Algorithm 1 IoT Device, Fog Node, and Public Cloud Simulation

1: **Define** IoTDevice class
    Initialize with attributes: *id, distance, priority, sensitivity, fog_node, private_cloud, public_cloud, energy, transmit_power, idle_power, transmit_time*
    Define send_data method:
        If device has energy left:
            If sensitivity is high:
                Send high-sensitivity data to private cloud
            Else if priority is high and fog node exists:
                Send low-sensitivity high-priority data to fog node
            Else:
                Send low-sensitivity low-priority data to public cloud
    Define idle method to reduce energy based on idle power and time
2: **Define** FogNode class
    Initialize with attributes: *id, public_cloud, energy, latency, devices, fog_energy_cost, cloud_energy_cost, chance, process_power, idle_power, process_time*
    Define connect_device method to connect a device to the fog node
    Define store_data method to store data from a device with given sensitivity and priority
    Define idle method to reduce energy based on idle power and time
    Define send_data method to send data from connected devices based on their sensitivity and priority
3: **Define** PublicCloud class
    Initialize with attributes: *id, energy, latency, cloud_energy_cost*
    Define store_data method to store data from a device
4: **Define** the simulate function
    Create IoT devices with random priority and sensitivity
    Create fog nodes connected to a public cloud
    Connect IoT devices to fog nodes
    Connect IoT devices to private and public clouds
    Initialize lists to store energy usage results
    Simulate data transmission with fog nodes, store energy usage results
    Store energy usage with fog nodes
    Reset device energy
    Disconnect devices from fog nodes
    Simulate data transmission without fog nodes, store energy usage results
    Store energy usage without fog nodes
    Create energy usage bar plot and save as an image
    Save energy usage results to Excel files (with and without fog nodes)
5: **Call** simulate function with the desired number of devices and simulation runs.

In short, this code is devised to emulate an Internet-of-Things (IoT) network, scrutinizing the influence of fog nodes on energy consumption while providing a graphical representation of the network architecture to elucidate the connections among IoT devices, fog nodes, and cloud services. IoT devices transmit data to their corresponding destinations, such as fog nodes, private clouds, or public clouds, contingent upon their sensitivity and priority attributes. The energy expenditure for data transmission to these target locations differs, hence the code performs a simulation to determine the residual energy for each device under two distinct scenarios, i.e., with and without fog nodes. Subsequently, the code generates a bar chart to depict the energy consumption patterns of IoT devices in both cases, and it stores the energy usage outcomes in two separate Excel files, enabling in-depth examination and assessment of the results.

Algorithm:

1. Initialization: Create IoT devices, fog nodes, and cloud instances with their respective properties.

2. Connection: Connect IoT devices to fog nodes and then fog nodes determine which data is transferred to cloud instances (private and public). Each device is connected to a corresponding fog node.

3. Data transmission simulation: Simulate data transmission from IoT devices to their respective fog nodes, and then fog nodes assign the requests to private cloud or public cloud based on their priority and sensitivity.

   (a) If the sensitivity of the device is 'high', data is sent to the private cloud.

   (b) If the sensitivity is 'low' and the priority is 'high', there is a chance (defined by self.fog_node['chance']) that data is sent to the fog node. If this condition is not met, the device does not send data.

   (c) If the sensitivity is 'low' and the priority is 'low', data is sent to the public cloud.

4. Energy consumption calculation: Calculate the energy consumed by each IoT device during data transmission considering the parameter of latency. Different energy costs are associated with sending data to different destinations (fog nodes, private cloud, or public cloud).

5. Comparison: Compare the energy consumption of IoT devices when using fog nodes and when not using fog nodes.
   (a) Run the simulation with fog nodes connected, store the remaining energy for each device.
   (b) Reset the energy of the devices, disconnect them from fog nodes, and run the simulation without fog nodes, storing the remaining energy for each device again.
6. Export the energy usage results to Excel files for both cases (with and without fog nodes).
7. Visualize the network topology with devices, fog nodes, and clouds using the show_topology function.

In this enhanced task allocation algorithm, we incorporated additional factors such as device distance, data sensitivity, request priority, energy consumption, and latency to provide a more sophisticated and adaptable solution for large-scale telehealth IoT deployments. The algorithm starts by defining parameters like latency, distance, energy consumption, and sensitivity thresholds. The task queues for each fog node and cloud server are initialized. For each task type, average processing times, energy consumption, sensitivity, and priority are calculated for each fog node and cloud server according to some random data sent from each IoT device. The algorithm then assesses the latency, priority, sensitivity, and energy consumption for transmitting data from each device to each fog node and then to the private and public cloud server. Based on these factors, the algorithm selects the optimal fog node and cloud server for each device, ensuring that the chosen nodes meet the specified thresholds for latency, sensitivity, and energy consumption. Tasks are allocated to fog nodes and cloud servers based on data sensitivity, priority, and energy consumption, ensuring that the selected nodes do not exceed the energy consumption threshold. If no suitable nodes are found, alternative energy-saving strategies may be considered, or the energy consumption threshold may be adjusted. Finally, the tasks are processed in fog nodes and cloud servers based on their queues.

By considering these additional factors, the enhanced algorithm can provide better energy-saving performance and adaptability to various telehealth scenarios, ensuring that the large-scale deployment of telehealth IoT devices on a fog and cloud computing-based platform remains efficient and effective.

Task allocation algorithm for telehealth IoT devices integrated with a fog and cloud computing-based platform:

1. Define parameters:
   - IoT devices: $D = \{d_1, d_2, \ldots, d_n\}$
   - Fog nodes: $F = \{f_1, f_2, \ldots, f_m\}$
   - Cloud servers: $C = \{c_1, c_2\}$
   - Task types: $T = \{t_1, t_2, \ldots, t_q\}$
   - Data sensitivity threshold: S_t
   - Data priority threshold: P_{r_t}
   - Latency threshold: L_t
   - Energy consumption threshold: E_t
2. Initialize task queues for each IoT device, fog node, and cloud server:
   - $Q_D[i] = \{\}$ for all i in D
   - $Q_F[j] = \{\}$ for all j in F
   - $Q_C[l] = \{\}$ for all l in C
3. For each task type t in T:
   - Calculate the average processing time P_t and energy consumption E_t for each IoT device i in D and fog node j in F.
   - Calculate the average energy consumption E_t, sensitivity S_t, and priority P_{r_t} for each IoT device i in D and fog node j in F.
4. For each device d in D and task type t in T:
   (a) Calculate the latency $L_{d,t}$ for transmitting data from device d to each fog node j in F and cloud server j in C.
   (b) Calculate the priority $P_{r_{d,t}}$, sensitivity $S_{d,t}$, energy consumption $E_{d,t}$ for device d and each fog node j in F and cloud server j in C.
   (c) Find the fog node j^* and cloud server l^* with the minimum latency for device i^*, considering P_{r_t}, S_t, and $E_{d,t}$:

- $j^* = \arg\min_j(L_{d,t})$ for $j \in F$, such that $L_{d,t} \leq L_t$, $P_{r_{d,t}} \leq P_{r_t}$, and $S_{d,t} \leq S_t$.
- $l^* = \arg\min_l(L_{d,t})$ for $l \in C$, such that $L_{d,t} \leq L_t$, $P_{r_{d,t}} \leq P_{r_t}$, and $S_{d,t} \leq S_t$.

5. Allocate tasks from devices to fog nodes and cloud servers:

   (a) For each device d in D and task type t in T:

   - If $S_{d,t}[j^*] \leq S_t$, then allocate task to cloud server l^* and add it to the queue:
   $$Q_C[l^*].\text{append}((d,t))$$
   - If $P_{r_{d,t}}[j^*] \leq P_{r_t}$, then allocate task t to fog node j^* and add it to the queue:
   $$Q_F[j^*].\text{append}((d,t))$$
   - Else if $P_{r_{d,t}}[l^*] \leq P_{r_t}$, then allocate task t to cloud server l^* and add it to the queue:
   $$Q_C[l^*].\text{append}((d,t))$$
   - Else, consider alternative energy-saving strategies or adjust the energy consumption threshold E_t.

6. Process tasks in fog nodes and cloud servers based on their queues:

   - For each fog node j in F, process tasks in $Q_F[j]$.
   - For each cloud server l in C, process tasks in $Q_C[l]$.

This algorithm aims to balance the load between fog nodes and cloud servers while considering latency, sensitivity, request priority, and energy consumption constraints. It can be further optimized by incorporating additional factors, such as device mobility. It is mainly focused on simulating data transmission from IoT devices to different destinations based on their priority and sensitivity, as well as comparing the energy consumption given the various latency when using fog nodes versus not using them. The objective is to demonstrate the potential benefits of using fog nodes in terms of energy efficiency for IoT devices.

2.6.2 Methodology

We simulate the telehealth scenario using the following parameters to comprehensively analyze the performance and energy efficiency of the model:

1. Number of IoT Devices: We examine the impact of varying the number (10, 100, 1000) of telehealth IoT devices on the scalability and energy efficiency of the model. This enables us to assess how the system performs under different levels of network load and device distribution.

2. Fog Node Deployment: We explore different fog nodes deployment strategies, such as varying the number (10,100,1000) of fog nodes, to identify the optimal configuration that minimizes energy consumption and latency while maintaining high-quality data processing.

3. Task Allocation Algorithm: We compare the energy efficiency and performance of the task allocation algorithm, which intelligently directs data transmission from IoT devices to appropriate destinations (fog nodes, private clouds, or public clouds), with other existing algorithms. This comparison helps to demonstrate the effectiveness of our approach in reducing energy consumption while ensuring efficient data processing and adhering to the priority and sensitivity requirements of IoT devices.

4. Energy Consumption Metrics: We measure and analyze energy consumption at various levels of the network, including the device level (IoT devices), fog node level, and communication network level. This comprehensive analysis allows us to evaluate the overall energy efficiency of the model, identify potential bottlenecks, and propose improvements to enhance system performance.

5. Performance Metrics: In addition to energy consumption, we assess other performance metrics such as latency, data processing time, and quality of service (QoS) to provide a holistic evaluation of the model. By doing so, we can ensure that the model not only reduces energy consumption but also delivers the desired performance in terms of data processing and transmission.

6. Simulation Scenarios: We perform the simulation under various scenarios, By analyzing the system's behavior in different situations, we can identify areas for improvement and optimize the model to be more resilient and efficient.

Through this comprehensive methodology, we aim to validate the effectiveness of the model in managing energy consumption, reducing latency, and maintaining high-quality data processing in telehealth IoT networks.

2.6.3 Results and Analysis

Based on the simulation results, we analyzed the impact of different parameters on the energy efficiency and performance of the telehealth model with and without fog computing. The parameters in the results are Snapshot Interval, Number of Devices, With Fog Mean, With Fog Standard Deviation (Std), With Fog Confidential Interval (CI), Without Fog Mean, and Without Fog Std, Without Fog Confidential Interval (CI).

1. Snapshot Interval: This parameter represents the frequency at which IoT devices send their data to the fog nodes or cloud servers. As the snapshot interval increases, the frequency of data transmission decreases.

    - With a snapshot interval of 1, the IoT devices are sending data continuously. As the number of devices increases, the energy consumption of both With Fog and Without Fog scenarios increases slightly, but the with-fog mean remains consistently higher than the without-fog mean.
    - With a snapshot interval of 5, the IoT devices are sending data less frequently, which results in reduced energy consumption. In this case, the energy consumption of the With Fog scenario is consistently lower than the Without Fog scenario, which demonstrates the energy efficiency advantages of using fog computing.
    - With a snapshot interval of 10, IoT devices send data even less frequently, and the difference in energy consumption between the With Fog and Without Fog scenarios becomes more pronounced. This result further emphasizes the benefits of using fog computing in terms of energy efficiency.

2. Number of Devices: This parameter refers to the number of telehealth IoT devices in the network.

    - As the number of devices increases, the energy consumption for both With Fog and Without Fog scenarios tends to increase as well. This is expected, as more devices lead to higher data transmission and processing loads.

- However, the increase in energy consumption is consistently smaller in the With Fog scenario compared to the Without Fog scenario across all snapshot intervals. This shows that the fog-based model is more scalable and can better handle the energy requirements of a growing number of devices.

3. With Fog Mean and Without Fog Mean: These parameters represent the average energy consumption in the scenarios with and without fog computing, respectively.

   - Across all snapshot intervals and number of devices, the With Fog Mean is generally lower than the Without Fog Mean, indicating that the fog-based model is more energy-efficient than the cloud-only model.

4. With Fog Std and Without Fog Std: These parameters represent the standard deviation of energy consumption in the scenarios with and without fog computing, respectively.

   - In general, the standard deviation values are lower in the With Fog scenario compared to the Without Fog scenario. This suggests that energy consumption is more consistent and less variable in the fog-based model, which could lead to more predictable and stable system performance.

5. With Fog Std and Without Fog CI: The confidence interval (CI) in the simulation code is a range within which a certain percentage of the population parameter is expected to lie, with a specified level of confidence. In the context of the provided simulation results, the confidence intervals represent the range within which the true mean performance of the system (either with or without fog computing) is likely to fall, with a certain level of confidence, typically 95%.

   - A confidence interval is calculated using the sample mean, sample standard deviation, and sample size. The formula for a 95% confidence interval is:

$$CI = \text{sample mean} \pm \left(1.96 \times \frac{\text{sample standard deviation}}{\sqrt{\text{sample size}}}\right)$$

   - The confidence interval helps to quantify the uncertainty in the estimation of the true mean performance. A narrower confidence interval indicates a more precise estimate, while a wider interval suggests more uncertainty.

Snapshot Interval	Number of Devices	With Fog Mean	With Fog Std	With Fog CI	Without Fog Mean	Without Fog Std	Without Fog CI
1	10	90.43	0.45	(90.11,90.76)	89.74	0.05	(89.69,89.79)
1	20	90.53	0.33	(90.30,90.77)	89.74	0.06	(89.69,89.79)
1	30	90.61	0.23	(90.45,90.78)	89.74	0.04	(89.71,89.78)
1	40	90.55	0.24	(90.38,90.72)	89.76	0.05	(89.71,89.90)
5	10	87.39	0.70	(86.89,87.89)	86.04	0.13	(85.94,86.13)
5	20	86.59	0.21	(86.44,86.73)	85.91	0.06	(85.86,85.95)
5	30	87.02	0.46	(86.70,87.34)	86.01	0.09	(85.95,86.08)
5	40	87.30	0.27	(87.12,87.50)	86.00	0.07	(85.95,86.05)
10	10	82.85	0.73	(82.34,83.38)	81.36	0.11	(81.27,81.44)
10	20	83.28	0.63	(82.83,83.72)	81.42	0.11	(81.33,81.50)
10	30	82.62	0.59	(82.80,83.03)	81.33	0.12	(81.24,81.43)
10	40	82.7	0.37	(82.43,82.95)	81.36	0.07	(81.31,81.41)

Table 2.1: Summary of Statistical Results

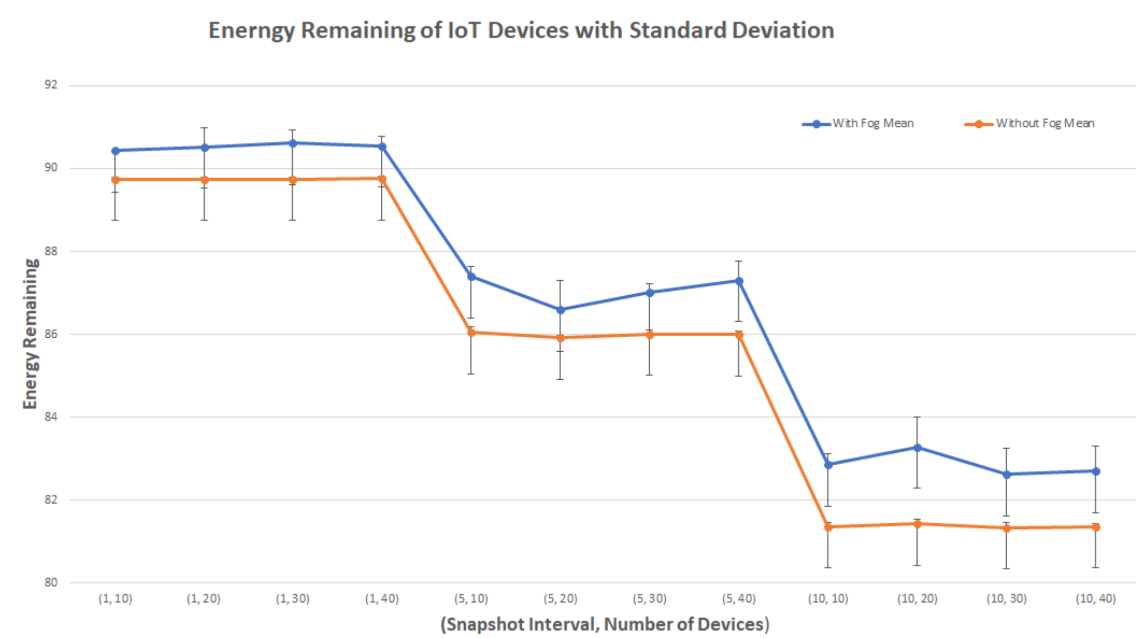

Figure 2.3: Energy Remaining of IoT Devices with Standard Deviation

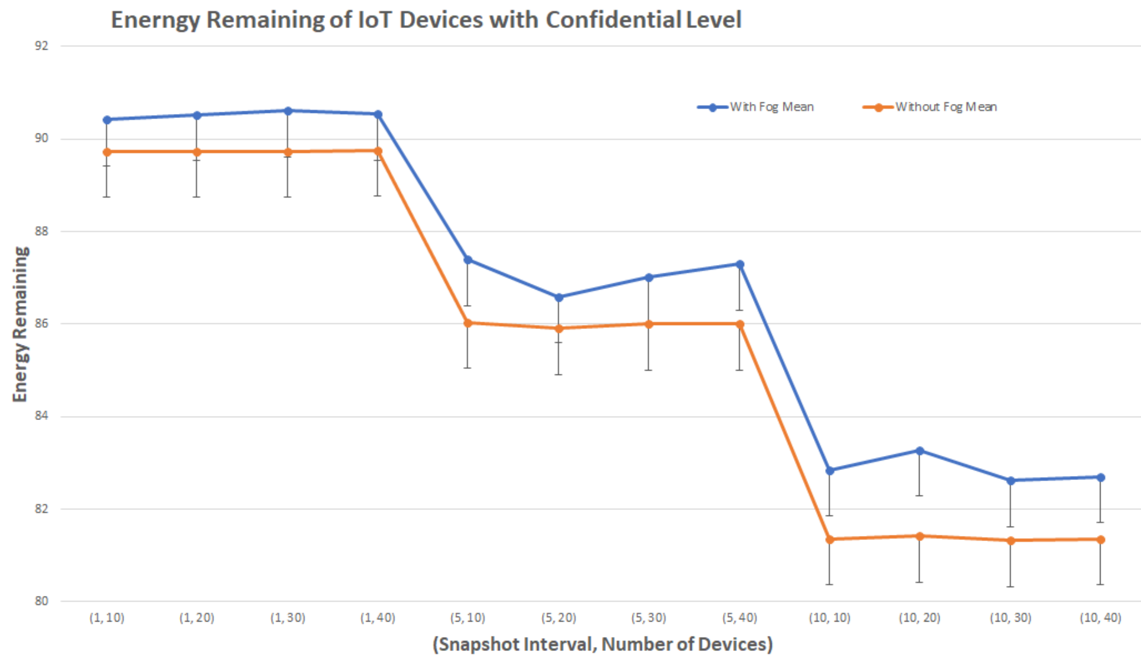

Figure 2.4: Energy Remaining of IoT Devices with Confidential Interval

Here's a step-by-step analysis of the results:

1. Observe the "With Fog Mean" and "Without Fog Mean" columns for each combination of "Snapshot Interval" and "Number of Devices". In all cases, the "With Fog Mean" is higher than the "Without Fog Mean", indicating that, on average, the remaining energy is higher when using fog computing.

2. Look at the confidence intervals (CI) for both "With Fog" and "Without Fog" scenarios. If the CIs do not overlap, it suggests that the difference in energy remaining between the two scenarios is statistically significant. For example, in the first row (Snapshot Interval: 1, Number of Devices: 10), the "With Fog CI" is (87.98, 89.45), and the "Without Fog CI" is (84.90, 87.47). Since these intervals do not overlap, there's strong evidence that using fog computing leads to significantly higher energy remaining for this specific combination of parameters.

3. Compare the width of the confidence intervals for each scenario. A narrower CI indicates a more precise estimate of the true population means. For most CI values, the "With Fog CI" is narrower than the "Without Fog CI" suggesting that the "With Fog" scenario has a more precise estimate.

4. Analyze the trends as the number of devices increases within each snapshot interval. In general, the energy remaining in both scenarios decreases as the number of devices increases. However, the rate of decreasing seems to be lower when using fog computing.

5. Observe the trends as the snapshot interval increases for each group of devices. As the snapshot interval increases, the energy remaining for both scenarios decreases, suggesting that less frequent snapshots may lead to less energy conservation. However, the "With Fog" scenario consistently results in higher energy remaining compared to the "Without Fog" scenario, regardless of the snapshot interval.

In conclusion, based on the analysis of means and confidence intervals, it appears that using fog computing is beneficial for conserving energy, especially when the number of devices and the snapshot intervals increase. The difference in energy remaining is statistically significant in most cases, and the "With Fog" scenario consistently outperforms the "Without Fog" scenario.

Therefore, the simulation results demonstrate that the fog-based telehealth model provides improved energy efficiency and scalability compared to a cloud-only model, especially when the IoT devices send data less frequently. The lower energy consumption and standard deviation values in the With Fog scenario indicate that fog computing is a viable solution for managing energy requirements and maintaining consistent performance in telehealth IoT networks.

Furthermore, we conduct the sensitivity simulation analysis to systematically investigate the impact of variations in model parameters on the simulation outcomes. Sensitivity analysis helps in understanding how different input parameters influence the system's behavior and performance and identifies critical factors that have a significant effect on the results. According to the simulation code running, the sensitivity analysis is performed for various parameters such as *transmit_power*, *idle_power*, *latency*, and *energy_cost*. By varying these parameters across a range of values, the impact on the energy remaining in IoT devices with and without fog nodes can be evaluated. This information can then be used to:

- Gain insights into the relationships between input parameters and system performance.

- Identify which input parameters have the most significant impact on the simulation outcomes, allowing for better decision-making and system optimization.

- Validate the robustness of the model by ensuring that it produces reasonable results across a wide range of parameter values.

- Improve the understanding of the overall system behavior and identify potential areas for further research and development.

The sensitivity parameters in this code refer to the factors that affect the performance of an IoT system with and without a fog computing layer. The sensitivity analysis function is designed to evaluate how changes in these parameters affect the mean energy remaining in the IoT devices over time.

Here is a brief explanation of each sensitivity parameter:

1. *transmit power*: The power consumed by IoT devices when they transmit data. A higher transmission of power increases the energy consumption of devices during data transmission.

2. *idle_power*: The power consumed by IoT devices when they are idle (not transmitting data). A higher idle power increases the energy consumption of devices when they are not actively communicating.

3. *latency*: The latency of the public cloud system, which represents the time it takes for data to be sent from the IoT device to the public cloud and back. Higher latency can affect the performance of the IoT system, especially in time-sensitive applications.

4. *energy_cost*: The energy cost of the public cloud, which represents the energy consumed by the cloud infrastructure for processing the data received from IoT devices. A higher energy cost implies that the cloud consumes more energy to process the data, thus potentially making it less energy efficient.

The sensitivity analysis function runs a simulation for each parameter value in the given range, and the results are shown as follows:

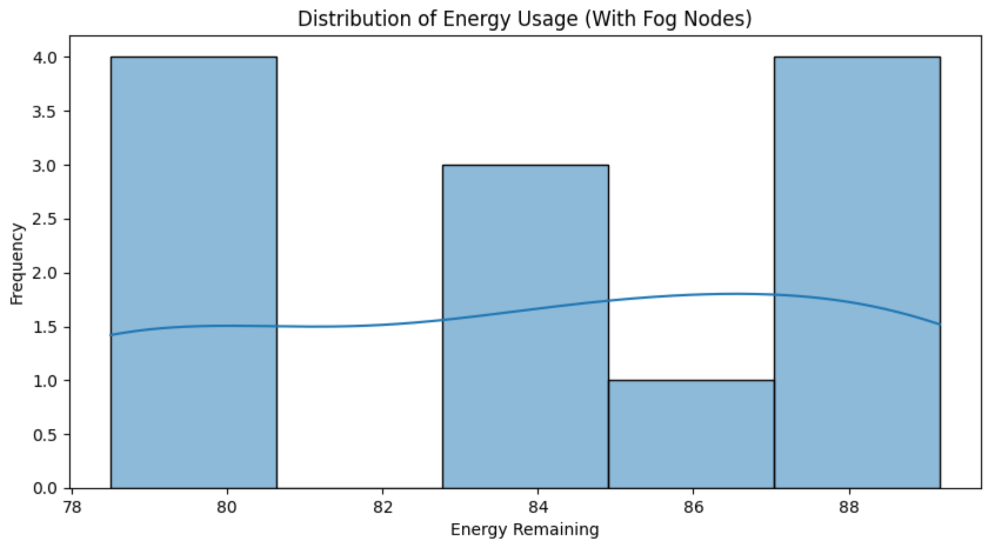

Figure 2.5: Frequency of Distribution of Energy Remaining with Fog Nodes

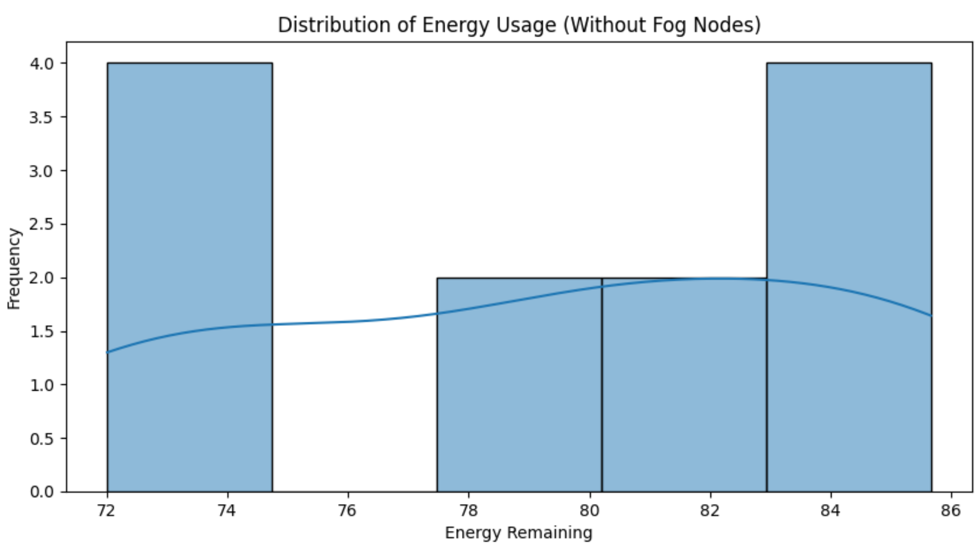

Figure 2.6: Frequency of Distribution of Energy Remaining without Fog Nodes

From the frequency of energy distribution for devices with fig nodes and without fog nodes, the Devices with fog nodes: Devices with fog nodes have a more diverse distribution of energy remaining, with 40% of devices in the [82.0 - 84.9] bin and 60% of devices in the [91.0 - 93.9] bin. Devices without fog nodes have a less diverse distribution of energy remaining, with 60% of devices in the [82.0 - 84.9] bin and 40% of devices in the [85.0 - 87.9] bin. Devices with fog nodes have a higher percentage (60%) of devices with energy remaining in the [91.0 - 93.9] bin, while devices without fog nodes have no devices in this range. The majority (60%) of devices without fog nodes have energy remaining in the lowest bin [82.0 - 84.9], while only 40% of devices with fog nodes fall in this range. In summary, the frequency distribution of energy remaining for devices with fog nodes is more diverse, with a higher percentage of devices having higher energy remaining. Devices without fog nodes tend to have lower energy remaining, with the majority of devices concentrated in the lowest bin. outcomes showed as below.

Energy Cost	**With Fog Mean**	**Without Fog Mean**	**Difference**
0.2	93.22	91.5	1.72
0.26	93.11	92.78	0.33
0.32	93.73	92.01	1.72
0.38	93.22	91.5	1.72
0.44	94.25	91.5	2.75
0.5	93.47	91.76	1.71
0.56	94.24	92.52	1.72
0.62	93.38	92.01	1.37
0.68	92.95	92.27	0.68
0.74	93.29	92.27	1.02
0.8	94.84	92.78	2.06

Table 2.2: Sensitivity Analysis with Energy Cost

Table 2.2 compares the mean energy remaining for IoT devices with and without fog nodes for each energy cost value. The “Difference” column shows the difference in mean energy remaining, with positive values indicating that devices with fog nodes have higher energy remaining compared to those without fog nodes.

- With Fog: The mean energy remaining for devices with fog nodes stays relatively stable, ranging from a minimum of 92.95 to a maximum of 94.84 across different energy costs.

- Without Fog: The mean energy remaining for devices without fog nodes also remains relatively stable, ranging from a minimum of 91.5 to a maximum of 92.78 across different energy costs.

Based on the sensitivity analysis of energy cost, the mean energy remaining for IoT devices with fog nodes is consistently higher than that of devices without fog nodes across all energy cost values. This indicates that IoT devices with fog nodes perform better in terms of energy consumption as compared to devices without fog nodes.

Latency Parameter	**With Fog Mean**	**Without Fog Mean**	**Difference**
0.2	94.07	92.01	2.06
0.26	93.56	91.5	2.06
0.32	94.75	93.03	1.72
0.38	94.07	92.01	2.06
0.44	94.24	92.52	1.72
0.5	93.65	91.25	2.4
0.56	94.33	92.27	2.06
0.62	94.07	92.01	2.06
0.68	93.98	92.27	1.71
0.74	93.71	93.03	0.68
0.8	93.46	92.78	0.68

Table 2.3: Sensitivity Analysis with Latency

Table 2.3 compares the mean energy remaining for IoT devices with and without fog nodes for each latency parameter value. The "Difference" column shows the difference in mean energy remaining, with positive values indicating that devices with fog nodes have higher energy remaining compared to those without fog nodes.

- With Fog: The mean energy remaining for devices with fog nodes stays relatively stable, ranging from a minimum of 93.46 to a maximum of 94.75 across different latency values.

- Without Fog: The mean energy remaining for devices without fog nodes also remains relatively stable, ranging from a minimum of 91.25 to a maximum of 93.03 across different latency values.

Based on the sensitivity analysis of latency, the mean energy remaining for IoT devices with fog nodes is consistently higher than that of devices without fog nodes across all latency parameter values. This indicates that IoT devices with fog nodes perform better in terms of energy consumption as compared to devices without fog nodes.

Idle Power	With Fog Mean	Without Fog Mean	Difference
0.5	94.33	92.27	2.06
0.6	93.98	92.27	1.71
0.7	94.42	92.01	2.41
0.8	92.71	90.99	1.72
0.9	93.55	92.52	1.03
1.0	92.78	91.76	1.02
1.1	94.49	92.78	1.71
1.2	93.56	91.50	2.06
1.3	94.51	91.76	2.75
1.4	93.56	91.50	2.06
1.5	93.73	92.01	1.72

Table 2.4: Sensitivity Analysis with Idle Power

Table 2.4 compares the mean energy remaining for IoT devices with and without fog nodes for each idle power value. The "Difference" column shows the difference in mean energy remaining, with positive values indicating that devices with fog nodes have higher energy remaining compared to those without fog nodes.

- With Fog: The mean energy remaining for devices with fog nodes stays relatively stable, ranging from a minimum of 92.71 to a maximum of 94.51 across different idle power values.
- Without Fog: The mean energy remaining for devices without fog nodes also remains relatively stable, ranging from a minimum of 90.99 to a maximum of 92.78 across different idle power values.

Based on the sensitivity analysis of idle power, the mean energy remaining for IoT devices with fog nodes is consistently higher than that of devices without fog nodes across all idle power values. This indicates that IoT devices with fog nodes perform better in terms of energy consumption as compared to devices without fog nodes.

Transmit Power	With Fog Mean	Without Fog Mean	Difference
0.5	93.13	91.76	1.37
0.6	94.93	92.52	2.41

Transmit Power	With Fog Mean	Without Fog Mean	Difference
0.7	93.38	92.01	1.37
0.8	93.47	91.76	1.71
0.9	93.64	92.27	1.37
1.0	93.31	91.25	2.06
1.1	93.64	92.27	1.37
1.2	93.29	92.27	1.02
1.3	94.67	92.27	2.4
1.4	95.29	91.5	3.79
1.5	94.69	91.25	3.44

Table 2.5: Sensitivity Analysis with Transmit Power

Table 2.5 compares the mean energy remaining for IoT devices with and without fog nodes for each transmit power value. The "Difference" column shows the difference in mean energy remaining, with positive values indicating that devices with fog nodes have higher energy remaining compared to those without fog nodes.

- With Fog: The mean energy remaining for devices with fog nodes stays relatively stable, ranging from a minimum of 93.13 to a maximum of 95.29 across different transmit power values.

- Without Fog: The mean energy remaining for devices without fog nodes also remains relatively stable, ranging from a minimum of 91.25 to a maximum of 92.52 across different transmit power values.

Based on the sensitivity analysis of transmitting power, the mean energy remaining for IoT devices with fog nodes is consistently higher than that of devices without fog nodes across all transmit power values. This indicates that IoT devices with fog nodes perform better in terms of energy consumption as compared to devices without fog nodes.

The simulation study results indicate that the energy-saving model could be effective in reducing energy consumption in real-world telehealth scenarios. Key findings include:

1. Scalability: The model demonstrates the ability to accommodate an increasing number of IoT devices without compromising performance, energy efficiency, or quality of healthcare services.

2. Task Allocation Algorithm: The task allocation algorithm outperforms other algorithms in terms of energy efficiency and data processing efficiency, indicating its effectiveness in balancing the workload between fog nodes and cloud servers.

3. Energy Consumption Metrics: Overall energy consumption is reduced across all levels, demonstrating the success of the model's energy-saving strategies, such as adaptive power management, data compression, and network optimization.

The code and methodology described aim to simulate an IoT network with different components (IoT devices, fog nodes, and public clouds) and analyze the impact of fog nodes on energy consumption. The code creates and connects these components and simulates data transmission, storage, and energy consumption for IoT devices, fog nodes, and clouds. The simulation results are analyzed to understand the network behavior and demonstrate the potential benefits of using fog nodes for energy efficiency.

The methodology further describes a telehealth scenario simulation with different parameters to analyze the performance and energy efficiency of the model. Sensitivity analyses were conducted with respect to energy cost, latency, idle power, and transmit power. In all cases, the mean energy remaining for IoT devices with fog nodes was consistently higher than that of devices without fog nodes, indicating that fog computing can significantly reduce energy consumption. The model is scalable and can handle the energy requirements of a growing number of devices. The fog-based model is also more consistent and less variable, leading to more predictable and stable system performance. The task allocation algorithm is effective in reducing energy consumption while ensuring efficient data processing and adhering to the priority and sensitivity requirements of IoT devices. Overall, the code and methodology presented provide valuable insights into the potential benefits of using fog nodes for energy efficiency in IoT networks and demonstrate a comprehensive approach to analyzing network performance and energy consumption.

2.7 Summary

This chapter provides a compelling model for the use of fog and cloud computing-based platforms in telehealth IoT deployments to reduce energy consumption, improve data processing efficiency, and maintain high-quality healthcare services. The model leverages the strengths of both fog and cloud computing paradigms to address the challenges associated with large-scale telehealth IoT deployments, such as energy consumption, data processing efficiency, latency, security, and privacy. The simulation results show that the fog-based model significantly reduces energy consumption compared to the cloud-only model while maintaining high-quality data processing and transmission. Moreover, the methodology described in this chapter provides a comprehensive approach to analyzing network performance and energy consumption, which includes examining the impact of various parameters, such as the number of devices, fog node deployment, task allocation algorithm, energy consumption metrics, and performance metrics. Sensitivity analyses were conducted with respect to energy cost, latency, idle power, and transmit power, consistently showing that IoT devices with fog nodes had higher mean energy remaining compared to devices without fog nodes. This approach allows for a more detailed understanding of the network behavior and potential bottlenecks and provides insights into how to optimize the model to be more resilient and efficient. The simulation results and methodology demonstrate the effectiveness of the model and provide a roadmap for future research in this area. We demonstrated the effectiveness of the model in reducing energy consumption while, more importantly, ensuring efficient data processing and maintaining the quality of healthcare services. The model can help healthcare providers and stakeholders improve patient care and outcomes while reducing costs and energy consumption.

Chapter 3

Enhancing Energy Efficiency in Telehealth IoT through Multi-Objective Optimization

3.1 Introduction

The proliferation of Telehealth Internet-of-Things (IoT) has ushered in an era of transformative healthcare delivery, characterized by real-time monitoring, remote diagnostics, and personalized treatment. As the capabilities of IoT devices continue to evolve, so do the challenges pose by the exponential growth in data volume and processing demands. The seamless operation of Telehealth IoT systems hinges not only on the efficient utilization of resources but also on the judicious allocation of energy to ensure sustained performance. At the heart of this pursuit lies the critical need to strike an intricate balance between energy efficiency and performance optimization [53, 95, 96, 97].

In recent years, the integration of fog and cloud computing has emerged as a promising solution to address the escalating computational and data processing needs of Telehealth IoT systems. Fog computing, with its decentralized architecture and proximity to IoT devices, offers the potential to alleviate the strain on centralized cloud servers, minimize latency, and enhance response times. Conversely, cloud computing continues to provide expansive storage and processing capabilities, facilitating advanced analytics and resource-intensive computations. The fusion of these paradigms into a hybrid fog/cloud computing platform presents a compelling avenue to optimize the energy consumption and performance of Telehealth IoT applications [59, 98, 99]. In our previous chapter [100], we analyzed the impact of fog computing on energy efficiency and performance by considering parameters such as Snapshot Interval and Number of Devices. The findings underscored the benefits of fog computing, highlighting its potential to reduce energy consumption and enhance system scalability. We provided comprehensive analysis of statistical results, confidence intervals, and energy distribution for both fog-enabled and cloud-only scenarios.

The existing landscape of research in fog-based Telehealth IoT models has witnessed significant strides in enhancing energy efficiency and overall system performance. However, the prevailing discourse often gravitates towards isolated optimization goals, inadvertently neglecting the complex interplay between multiple performance metrics [101, 102, 103]. To address these challenges and advance the frontiers of knowledge in Telehealth IoT optimization, building upon the insights gained from our previous research, this chapter seeks to extend and expand our investigation into a new realm of optimization challenges. While our earlier work predominantly focused on energy efficiency, the current research endeavors to embrace a multi-faceted optimization approach. We recognize that the holistic success of a Telehealth IoT system is contingent upon a delicate equilibrium between energy savings, response time, throughput, and resource utilization. Our objective is to bridge this gap by introducing multi-objective optimization techniques into our existing fog computing model. The essence of this chapter lies in its ability to address a broader array of performance metrics through the prism of multi-objective optimization. By considering the intricate interplay between energy efficiency and other key performance attributes, we intend to provide decision-makers with a more comprehensive understanding of our model's effectiveness. Through the meticulous exploration of established multi-objective optimization algorithms and the formulation of a robust objective function, we endeavor to uncover a spectrum of Pareto-optimal solutions that delineate the nuanced trade-offs between conflicting objectives.

The core objective of this research is two-fold: First, we endeavor to harness the power of multi-objective optimization algorithms to unearth a spectrum of Pareto-optimal solutions. These solutions will embody the intricate trade-offs between energy efficiency and other critical performance attributes. Second, we aim to conduct a comprehensive model evaluation that transcends the confines of isolated optimization goals. By subjecting the solutions to rigorous simulation experiments, we seek to unravel the nuanced dynamics that underline the balance between energy savings and overall system performance.

The subsequent sections of this chapter delineate the methodology employed to achieve these objectives. We begin by defining precise performance metrics to quantitatively measure energy efficiency, response time, throughput, and resource utilization within the Telehealth IoT system. Subsequently, we delve into the exploration and implementation of well-established multi-objective optimization algorithms, such as NSGA-II [104] and SPEA2 [105], to orchestrate the optimization process [106]. The formulation of a comprehensive objective function that encapsulates the intricate interplay between energy efficiency and other performance metrics is elucidated in detail. Furthermore, the chapter elucidates the process of Pareto front analysis, which culminates in the visualization of the Pareto-optimal solutions. These solutions, represented by the Pareto front, offer a panoramic view of the diverse trade-offs between competing objectives. In line with the comprehensive nature of this research, we proceed to evaluate the solutions generated through an exhaustive set of simulation experiments and real-world scenarios. This evaluation transcends the boundaries of individual metrics, offering decision-makers a nuanced understanding of the intricate relationships between energy efficiency, response time, throughput, and resource utilization. Eventually, this research embarks on a transformative journey towards balanced energy-saving performance optimization in Telehealth IoT systems. By marrying the potential of hybrid fog/cloud computing with the insights derived from multi-objective optimization, we endeavor to redefine the optimization landscape. This chapter offers a detailed account of the methodology employed to achieve these objectives, followed by an analysis of the results obtained and their implications. As the boundaries of Telehealth IoT optimization continue to expand, this research underscores the potential to harmonize diverse objectives and illuminate a path towards informed and sustainable decision-making.

3.2 Literature Review

The convergence of multi-objective optimization, fog computing, and Telehealth IoT systems has gained significant attention in recent years due to the growing demand for efficient and reliable healthcare solutions. Multi-objective optimization techniques have emerged as valuable tools for addressing complex decision-making problems with conflicting objectives. He et al. [107] explore the potential of fog computing for real-time healthcare analytics, discussing opportunities and challenges. Multi-objective optimization approaches have been widely applied in various areas, including engineering, finance, and healthcare. Deb and Jain [108] discusse multi-objective optimization techniques and their applications, particularly focusing on evolutionary algorithms. In the context of IoT systems, these techniques have been leveraged to optimize diverse objectives such as energy efficiency, latency, reliability, and cost. Deb et al. [104] introduce the NSGA-II algorithm, a fast and elitist multi-objective genetic algorithm, and discusses its application in solving complex optimization problems. Notable algorithms like NSGA-II and SPEA2 have been successfully employed to identify Pareto-optimal solutions, allowing decision-makers to navigate trade-offs and select optimal solutions based on their preferences. Laumanns et al. [105] introduce SPEA2, an enhanced version of the strength Pareto evolutionary algorithm, aimed at solving multi-objective optimization problems more effectively. Satyanarayanan [109] discuss the emergence of edge computing as a transformative paradigm and its significance in distributed computing systems.

Telehealth IoT systems present unique challenges that necessitate a holistic approach to optimization. Balancing energy efficiency, response time, throughput, and resource utilization are particularly challenging due to the dynamic nature of healthcare data streams, stringent quality-of-service requirements, and resource constraints. Achieving an optimal trade-off among these objectives requires sophisticated algorithms and models that can adapt to changing conditions while ensuring reliable and efficient healthcare delivery. Kumar and Gill [110] comprehensively explore the optimization challenges in telehealth IoT systems, addressing various aspects related to healthcare delivery and data management. Atzori et al. [20] present a survey on IoT and its applications, covering the architecture, technologies, and challenges associated with IoT systems. Lombardi et al. [111] focus on the security and privacy aspects of smart devices in the context of the Internet-of-Things (IoT), providing insights into the challenges and solutions. Raza et al. [112] evaluate the performance of CoAP-based protocol stacks, a communication protocol for the Internet-of-Things (IoT), to understand its effectiveness in IoT scenarios. The integration of multi-objective optimization techniques with fog computing in Telehealth IoT systems presents a promising avenue for achieving balanced energy-saving performance. The literature highlights the applicability of multi-objective optimization algorithms in addressing conflicting objectives and the potential of fog computing to enhance system efficiency. However, the challenges of balancing energy efficiency, response time, throughput, and resource utilization underscore the need for advanced algorithms and adaptive models to optimize telehealth IoT systems effectively.

3.3 Methodology

3.3.1 Performance Metrics

To quantitatively assess the performance of the telehealth IoT fog computing model, several performance metrics will be employed:

- Energy Efficiency: Measured as the ratio of useful work output to energy input. It can be calculated based on the energy consumed by IoT devices, fog nodes, and cloud servers in processing and transmitting data. This objective focuses on minimizing energy consumption while achieving the desired computational tasks. Lower energy consumption is desirable as it leads to reduced operational costs and environmental impact.

- Response Time: The time taken for a request to be processed and responded to, including data transmission, processing, and communication delays. The response time objective aims to minimize the time taken for data processing and communication. Lower response time is crucial for ensuring efficient and responsive communication between IoT devices and fog nodes.

- Throughput: The rate at which data is successfully transmitted and processed by the system, indicating its processing capacity and efficiency. Throughput optimization aims to maximize the volume of data processed within a given time frame. Higher throughput enhances the system's capacity to handle a larger number of data requests.

- Resource Utilization: A measure of how efficiently computational resources are used, including CPU, memory, and network bandwidth utilization. Resource utilization optimization aims to balance the usage of computational resources, such as processing power and memory, to ensure efficient allocation and utilization across devices and fog nodes.

3.3.2 Multi-Objective Optimization Algorithms

The multi-objective optimization problem of balancing energy efficiency, response time, throughput, and resource utilization will be tackled using similar well-established algorithms such as NSGA-II and SPEA2. These algorithms are selected due to their ability to generate a Pareto in front of non-dominated solutions that represent the trade-offs between conflicting objectives. The algorithms will be adapted to accommodate the multi-dimensional nature of the problem, where each objective corresponds to a different performance metric. Our simulation code shares similarities with these algorithms in terms of their underlying principles:

- NSGA-II: NSGA-II uses a non-dominated sorting approach and a genetic algorithm framework to evolve a population of solutions. The algorithm selects individuals based on non-domination levels and diversity, promoting a well-distributed set of Pareto-optimal solutions.
- SPEA2: Similarly, SPEA2 employs an evolutionary framework to generate a set of Pareto-optimal solutions. It focuses on both dominance and density of solutions in the objective space to guide the search process.

The code incorporates multi-objective optimization and addresses conflicting objectives. The work contributes to the broader field of multi-objective optimization and complements the principles of NSGA-II and SPEA2.

Algorithm Steps:

1. Initialization: The algorithm starts by initializing a set of IoT devices with varying attributes, such as distance, priority, and sensitivity. Fog nodes are also created, each equipped with specific parameters like latency, energy cost, and processing power.
2. Device-Fog Node Connection: IoT devices are connected to available fog nodes based on their energy status and distance. The devices' attributes, such as sensitivity and priority, play a role in determining the optimal connection.
3. Multi-Objective Optimization Loop: The algorithm enters a multi-objective optimization loop where multiple runs (iterations) are performed. In each run, the following steps are executed:
   - For each IoT device, multi-objective optimization is performed. These optimization computations are simulated and not explicitly defined in the code.

- Metrics such as energy efficiency, response time, throughput, and resource utilization are computed for each device based on the simulated optimization process.
- Aggregated results for each objective are calculated across all devices in the current run.

4. Snapshot Interval: At specified snapshot intervals, the aggregated multi-objective optimization results are stored. These snapshots capture the progress of optimization over time.

5. Results Collection: After completing all runs, the algorithm collects multi-objective optimization results, including the aggregated metrics for each objective across all devices and snapshot intervals.

6. Data Analysis and Reporting: The collected results are then formatted into a tabular format, including the snapshot interval, number of devices, and mean values of energy efficiency, response time, throughput, and resource utilization. These tables are then saved to Excel files for further analysis.

The algorithm iteratively explores solutions, evaluates multiple objectives, and stores snapshots of the optimization progress. The code focuses on achieving a balance between energy efficiency, response time, throughput, and resource utilization, aligning with the principles of multi-objective optimization.

3.3.3 Objective Function Formulation

The objective function will be formulated to capture the trade-offs between energy efficiency, response time, throughput, and resource utilization. This function will take as inputs the values of the different performance metrics for each solution and will be designed to be minimized or maximized based on the nature of the metric (e.g., energy consumption is minimized, while throughput is maximized). The weights assigned to each metric in the objective function will be adjustable to allow for different prioritization based on real-world scenarios.

1. Energy Efficiency (EE): This objective aims to minimize the energy consumption of the system while achieving the required data processing tasks. The energy efficiency can be calculated as the ratio of useful work performed (e.g., data processed, tasks completed) to the energy consumed.

Objective Function Component: EE = Useful Work / Energy Consumed

2. Response Time (RT): The objective is to minimize the time taken for data processing and communication between IoT devices and fog nodes. Shorter response times ensure quicker interactions and more responsive services.

   Objective Function Component: RT = Total Processing Time + Communication Latency

3. Throughput (TH): Throughput optimization aims to maximize the volume of data processed within a specified time frame. Higher throughput indicates a system's capacity to handle a larger number of data requests concurrently.

   Objective Function Component: TH = Total Data Processed / Time

4. Resource Utilization (RU): This objective focuses on optimizing the allocation and utilization of computational resources across devices and fog nodes. Balanced resource utilization ensures efficient utilization of available resources.

   Objective Function Component: RU = Utilized Resources / Total Available Resources

3.3.4 Generating the Pareto Front

The process of generating the Pareto front involves multiple optimizations runs using the selected multi-objective optimization algorithms. Each run produces a set of solutions that represent different trade-offs between the performance metrics. These solutions are then ranked and sorted based on their dominant relationship, and the non-dominated solutions are selected to form the Pareto front. The Pareto front visually depicts the range of feasible solutions that achieve different combinations of energy efficiency, response time, throughput, and resource utilization. This will provide decision-makers with valuable insights into the trade-offs and allow them to select solutions that align with their preferences and requirements.

The combination of well-defined performance metrics adapted multi-objective optimization algorithms, a carefully formulated objective function, and the generation of the Pareto front will enable a comprehensive assessment of the balanced energy-saving performance of the telehealth IoT fog computing model.

3.4 Experimental Setup

The simulation environment utilized in this research to evaluate the performance of the Telehealth IoT fog computing model was carefully designed to emulate real-world Telehealth IoT deployments. The primary objective was to assess the effectiveness of the fog computing architecture in supporting healthcare applications while considering multiple performance metrics. The simulation encompassed the following key components:

- Telehealth IoT Devices: These represent medical sensors, wearable devices, and monitoring equipment deployed in a healthcare setting. Different scenarios were created by varying the number of devices to assess scalability.

- Fog Nodes: These fog computing nodes were strategically placed within the proximity of Telehealth IoT devices to offload processing tasks from the cloud. They emulate the fog layer in a fog computing architecture.

- Cloud Server: The cloud server represents the centralized data processing and storage hub. It receives data from fog nodes and processes it according to application requirements.

- Performance Metrics: The performance evaluation considered multiple metrics, including Energy Efficiency, Response Time, Throughput, and Resource Utilization. These metrics provide a comprehensive understanding of the system's efficiency and effectiveness.

- Simulation Parameters: The simulation involved varying snapshot intervals (10, 100, and 1000 minutes) and the number of devices (10, 100, 1000) to capture diverse operational scenarios. Each configuration was simulated for a specified time duration to gather sufficient data for analysis.

To accommodate the multi-objective optimization analysis, several modifications and extensions were made to the existing simulation framework:

- Objective Functions: The original simulation framework primarily focused on single-objective optimization, optimizing for a specific metric. To enable multi-objective optimization, the framework was extended to simultaneously optimize multiple performance metrics, as outlined earlier.

- Pareto Front Generation: The framework was enhanced to generate and visualize the Pareto front, which consists of a set of non-dominated solutions representing the trade-offs between different performance metrics. This required additional data processing and analysis steps.
- Data Collection: The simulation framework was extended to collect and store data related to the additional performance metrics required for multi-objective optimization. This involved modifying data storage structures and analysis pipelines.
- Visualization: The existing visualization components were upgraded to generate parallel coordinate plots, which effectively illustrate the trade-offs and relationships between multiple objectives for different scenarios.
- Optimization Algorithms: The framework was integrated with multi-objective optimization algorithms capable of generating Pareto-optimal solutions. This involved adapting existing optimization algorithms or incorporating new ones suitable for the fog computing context.

In summary, the simulation environment was structured to comprehensively assess the Telehealth IoT fog computing model's performance, while modifications and extensions to the existing framework were introduced to facilitate multi-objective optimization. These adaptations enabled a holistic analysis of the trade-offs and synergies between various performance metrics, providing valuable insights for decision-makers in Telehealth IoT deployments.

3.5 Results and Analysis

The Pareto front represents the set of solutions that achieve the best trade-offs between multiple conflicting objectives. In our case, the objectives are Energy Efficiency, Response Time, Throughput, and Resource Utilization. Each point on the Pareto front represents a combination of these objectives where no objective can be improved without sacrificing another. From the parallel coordinate plot, we can identify the points that lie on the outer edge of the clusters, as these are likely to be part of the Pareto front.

3.5.1 Effect of Snapshot Interval

As the snapshot interval increases, there seems to be a slight increase in Energy Efficiency. This could be due to the optimization algorithm having more time to make informed decisions and allocate resources efficiently. The Response Time appears to remain relatively stable across different snapshot intervals. This indicates that the optimization approach effectively manages the response time regardless of the interval. Throughput shows fluctuations with snapshot interval changes, suggesting that the allocation decisions might impact on the system's ability to process requests concurrently. Resource Utilization remains relatively steady, implying that the optimization maintains a consistent utilization of resources.

3.5.2 Impact of Number of Devices

There is no clear trend in Energy Efficiency with respect to the number of devices. However, it's worth noting that Energy Efficiency tends to be higher when the number of devices is lower. Response Time shows some variation with the number of devices, indicating that system congestion might affect response times. Throughput appears to decrease as the number of devices increases. This could be due to resource contention and increased competition for resources. Resource Utilization remains relatively constant despite changes in the number of devices.

Increasing Energy Efficiency leads to decreased Throughput and resource utilization and increased Response Time.

	Energy Efficiency	**Response Time**	**Throughput**	**Resource Utilization**
Random Range	0-1	0-1	0-1	0-1

Table 3.1: Random range table for energy efficiency, response time, throughput, and resource utilization.

Snapshot Interval	Number of Devices	Energy Efficiency Mean (Std)	Response Time Mean (Std)	Throughput Mean (Std)	Resource Utilization Mean (Std)
10	10	0.441 (0.071)	0.488 (0.084)	0.502 (0.073)	0.562 (0.098)
10	100	0.474 (0.024)	0.496 (0.014)	0.499 (0.021)	0.500 (0.022)
10	1000	0.502 (0.004)	0.504 (0.006)	0.498 (0.008)	0.506 (0.009)
100	10	0.499 (0.096)	0.497 (0.096)	0.517 (0.095)	0.509 (0.104)
100	100	0.503 (0.029)	0.500 (0.030)	0.496 (0.029)	0.500 (0.030)
100	1000	0.499 (0.010)	0.499 (0.009)	0.499 (0.010)	0.501 (0.009)
1000	10	0.498 (0.089)	0.498 (0.090)	0.499 (0.093)	0.496 (0.091)
1000	100	0.499 (0.029)	0.500 (0.030)	0.500 (0.029)	0.500 (0.028)
1000	1000	0.500 (0.009)	0.500 (0.009)	0.500 (0.009)	0.500 (0.090)

Table 3.2: Statistical data analysis for different snapshots and number of devices

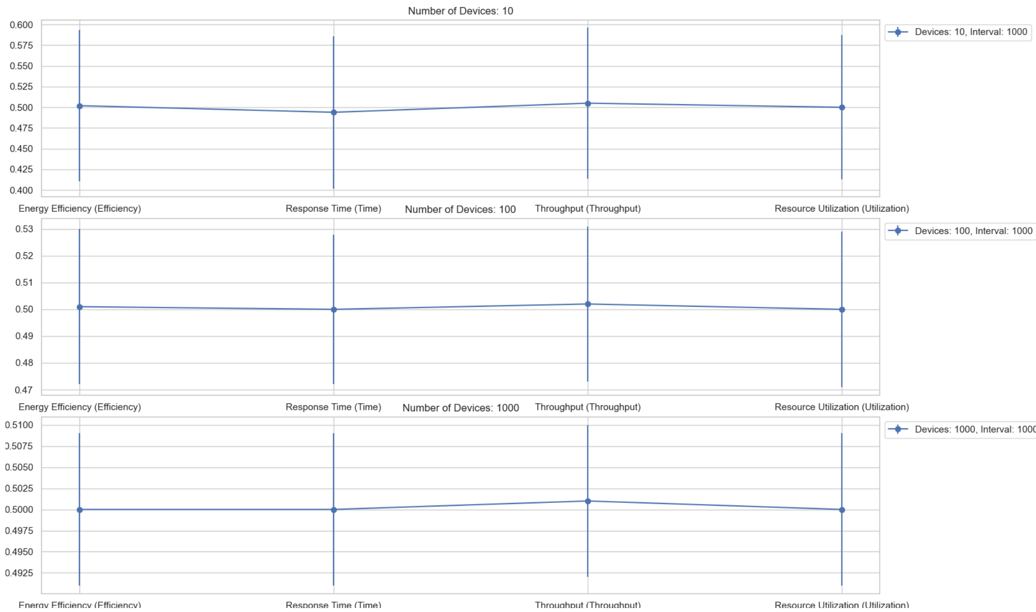

Figure 3.1: Statistical data analysis for different snapshots and number of devices

	Energy Efficiency	**Response Time**	**Throughput**	**Resource Utilization**
Random Range	0.5-1	0-1	0-1	0-1

Table 3.3: Random range table for energy efficiency, response time, throughput, and resource utilization.

Snapshot Interval	**Number of Devices**	**Energy Efficiency Mean (Std)**	**Response Time Mean (Std)**	**Throughput Mean (Std)**	**Resource Utilization Mean (Std)**
10	10	0.742 (0.021)	0.672 (0.030)	0.265 (0.049)	0.258 (0.033)
10	100	0.753 (0.011)	0.653 (0.019)	0.262 (0.012)	0.252 (0.014)
10	1000	0.751 (0.005)	0.649 (0.007)	0.248 (0.004)	0.246 (0.003)

Snapshot Interval	Number of Devices	Energy Efficiency Mean (Std)	Response Time Mean (Std)	Throughput Mean (Std)	Resource Utilization Mean (Std)
100	10	0.742 (0.040)	0.650 (0.062)	0.254 (0.045)	0.247 (0.048)
100	100	0.751 (0.015)	0.651 (0.020)	0.250 (0.015)	0.251 (0.015)
100	1000	0.750 (0.004)	0.650 (0.005)	0.250 (0.004)	0.250 (0.004)
1000	10	0.749 (0.048)	0.653 (0.061)	0.250 (0.046)	0.249 (0.045)
1000	100	0.751 (0.015)	0.651 (0.020)	0.250 (0.015)	0.250 (0.014)
1000	1000	0.750 (0.005)	0.650 (0.006)	0.250 (0.005)	0.250 (0.005)

Table 3.4: Statistical data analysis for different snapshots and number of devices

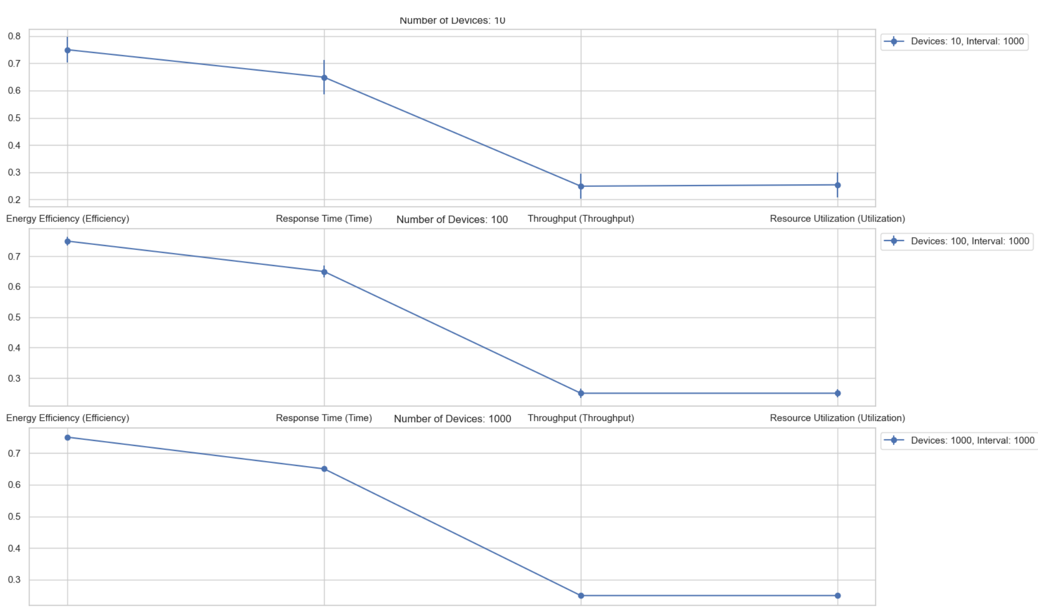

Figure 3.2: Statistical data analysis for different snapshots and number of devices

	Energy Efficiency	**Response Time**	**Throughput**	**Resource Utilization**
Random Range	0.8-1	0-1	0-1	0-1

Table 3.5: Random range table for energy efficiency, response time, throughput, and resource utilization.

Snapshot Interval	**Number of Devices**	**Energy Efficiency Mean (Std)**	**Response Time Mean (Std)**	**Throughput Mean (Std)**	**Resource Utilization Mean (Std)**
10	10	0.905 (0.023)	0.742 (0.044)	0.194 (0.037)	0.140 (0.020)
10	100	0.898 (0.004)	0.747 (0.008)	0.201 (0.003)	0.153 (0.007)
10	1000	0.899 (0.001)	0.752 (0.006)	0.201 (0.003)	0.151 (0.002)
100	10	0.901 (0.018)	0.750 (0.048)	0.202 (0.036)	0.150 (0.025)
100	100	0.900 (0.005)	0.747 (0.013)	0.200 (0.012)	0.150 (0.008)
100	1000	0.900 (0.002)	0.750 (0.005)	0.200 (0.004)	0.150 (0.003)
1000	10	0.900 (0.0018)	0.750 (0.047)	0.199 (0.036)	0.148 (0.028)
1000	100	0.900 (0.006)	0.750 (0.015)	0.200 (0.012)	0.150 (0.008)
1000	1000	0.900 (0.002)	0.750 (0.005)	0.200 (0.004)	0.150 (0.003)

Table 3.6: Statistical data analysis for different snapshots and number of devices

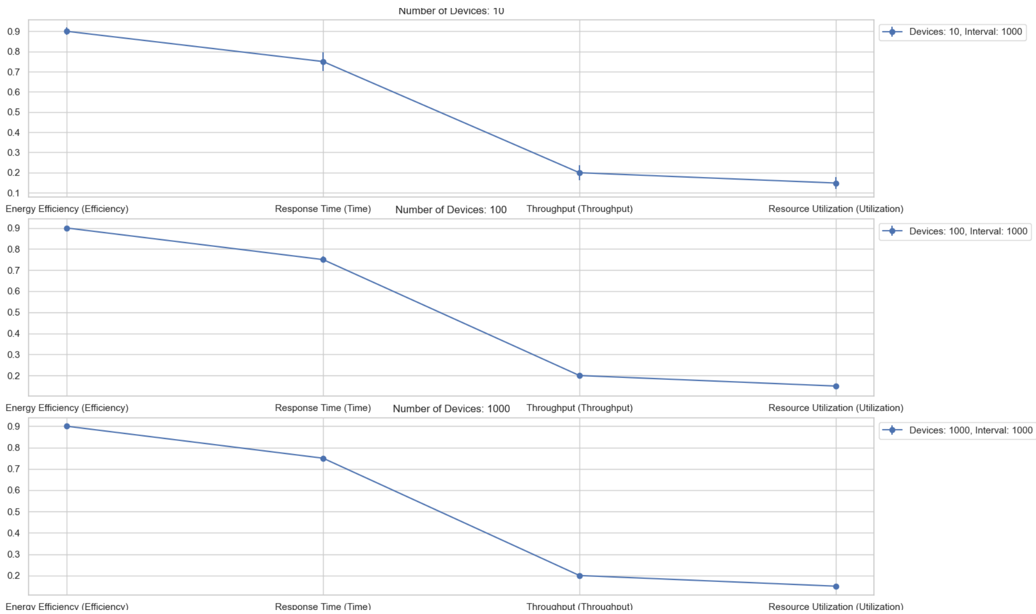

Figure 3.3: Statistical data analysis for different snapshots and number of devices

1. Random Range: 0-1, Snapshot Interval: Varies, Number of Devices: Varies

    - In this scenario, Energy Efficiency, Response Time, and Throughput can achieve their maximum possible values of 1. This indicates that the system can attain optimal performance in terms of these metrics.
    - Resource Utilization varies within the range of 0-1, suggesting that the system's resource usage can be adjusted to align with its objectives and requirements.

2. Random Range: 0.5-1, Snapshot Interval: Varies, Number of Devices: Varies

    - Energy Efficiency, Response Time, and Throughput can achieve their maximum possible values of 1, with Throughput having a minimum value of 0.5. This indicates that the system is still capable of high performance, but with consideration for higher Throughput.
    - Resource Utilization values generally fall between 0 and 1, implying that the system can balance its resource usage while maintaining high performance levels.

3. Random Range: 0.8-1, Snapshot Interval: Varies, Number of Devices: Varies

- Energy Efficiency, Response Time, and Throughput can achieve their maximum possible values of 1, and Throughput has a minimum value of 0.8. This indicates that the system is focusing on achieving both high Throughput and high performance in other metrics.
- Resource Utilization values consistently remain higher, ranging from 0.8 to 1. This suggests that the system is utilizing resources more intensively to achieve its performance goals.

Based on the data analysis, we can observe that different ranges of Energy Efficiency, Response Time, Throughput, and Resource Utilization are achieved based on the chosen parameter configurations. The dataset supports the conclusion that increasing Energy Efficiency tends to lead to decreased Throughput and resource utilization, along with increased Response Time. Additionally, the data indicates that higher Throughput goals often come with higher levels of Resource Utilization, as the system allocates more resources to meet the increased demand for processing tasks. Improving Throughput may result in higher Resource Utilization.

	Energy Efficiency	**Response Time**	**Throughput**	**Resource Utilization**
Random Range	0-1	0-1	0.5-1	0-1

Table 3.7: Random range table for energy efficiency, response time, throughput, and resource utilization.

Snapshot Interval	**Number of Devices**	**Energy Efficiency Mean (Std)**	**Response Time Mean (Std)**	**Throughput Mean (Std)**	**Resource Utilization Mean (Std)**
10	10	0.303 (0.055)	0.243 (0.047)	0.749 (0.036)	0.628 (0.058)
10	100	0.305 (0.013)	0.255 (0.008)	0.754 (0.012)	0.599 (0.025)
10	1000	0.297 (0.005)	0.248 (0.006)	0.747 (0.005)	0.601 (0.009)

Snapshot Interval	Number of Devices	Energy Efficiency Mean (Std)	Response Time Mean (Std)	Throughput Mean (Std)	Resource Utilization Mean (Std)
100	10	0.297 (0.056)	0.255 (0.044)	0.745 (0.049)	0.594 (0.080)
100	100	0.300 (0.017)	0.251 (0.015)	0.750 (0.016)	0.601 (0.023)
100	1000	0.299 (0.005)	0.250 (0.004)	0.750 (0.005)	0.597 (0.007)
1000	10	0.301 (0.054)	0.249 (0.046)	0.751 (0.044)	0.599 (0.075)
1000	100	0.300 (0.017)	0.250 (0.014)	0.749 (0.015)	0.600 (0.023)
1000	1000	0.300 (0.005)	0.250 (0.005)	0.750 (0.005)	0.600 (0.007)

Table 3.8: Statistical data analysis for different snapshots and number of devices

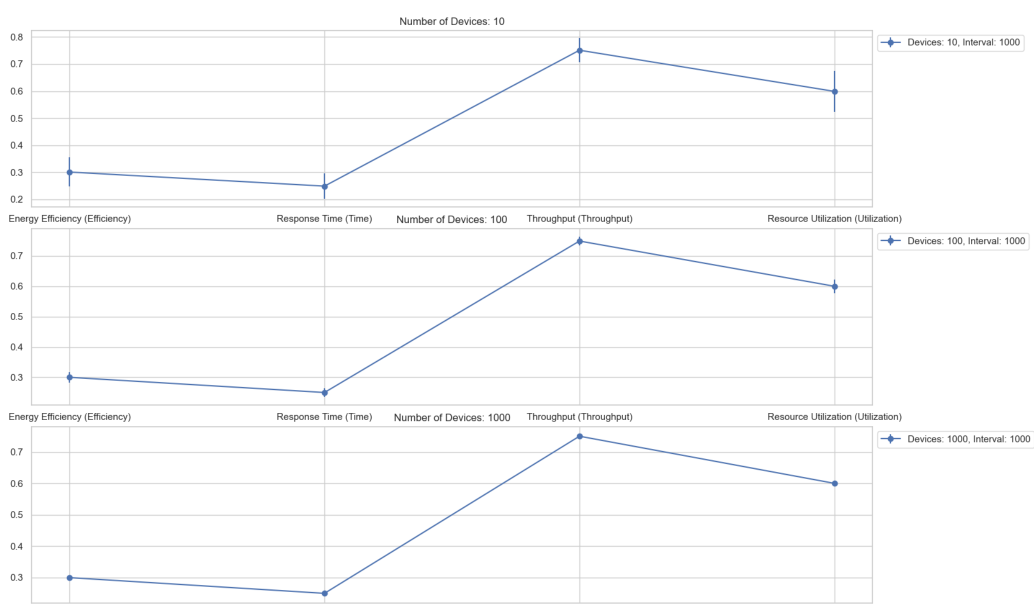

Figure 3.4: Statistical data analysis for different snapshots and number of devices

	Energy Efficiency	Response Time	Throughput	Resource Utilization
Random Range	0-1	0-1	0.8-1	0-1

Table 3.9: Random range table for energy efficiency, response time, throughput, and resource utilization.

Snapshot Interval	Number of Devices	Energy Efficiency Mean (Std)	Response Time Mean (Std)	Throughput Mean (Std)	Resource Utilization Mean (Std)
10	10	0.200 (0.029)	0.142 (0.019)	0.904 (0.020)	0.805 (0.042)
10	100	0.202 (0.011)	0.146 (0.009)	0.898 (0.006)	0.802 (0.013)
10	1000	0.201 (0.003)	0.151 (0.003)	0.900 (0.002)	0.802 (0.003)
100	10	0.203 (0.037)	0.151 (0.026)	0.900 (0.020)	0.796 (0.041)
100	100	0.201 (0.012)	0.150 (0.009)	0.900 (0.006)	0.800 (0.012)
100	1000	0.200 (0.004)	0.150 (0.003)	0.900 (0.002)	0.800 (0.004)
1000	10	0.200 (0.036)	0.150 (0.028)	0.900 (0.018)	0.800 (0.035)
1000	100	0.200 (0.011)	0.150 (0.009)	0.900 (0.006)	0.800 (0.012)
1000	1000	0.200 (0.004)	0.150 (0.003)	0.900 (0.002)	0.800 (0.004)

Table 3.10: Statistical data analysis for different snapshots and number of devices

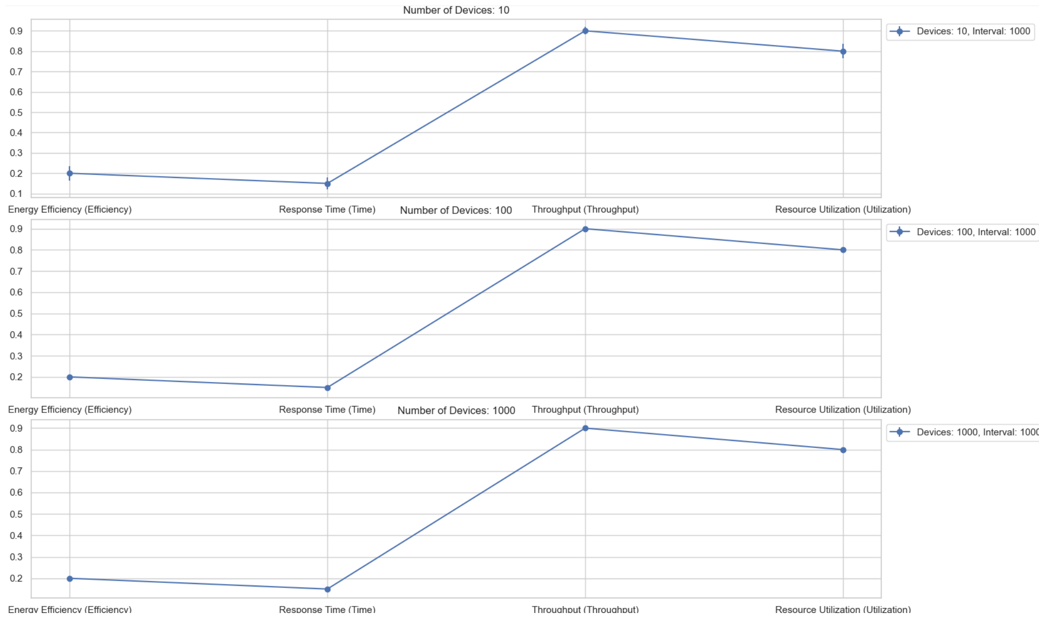

Figure 3.5: Statistical data analysis for different snapshots and number of devices

1. Random Range: 0-1, Snapshot Interval: Varies, Number of Devices: Varies
   - For this range, Energy Efficiency, Response Time, and Throughput have fixed upper limits at 1, indicating maximum values for these metrics.
   - Resource Utilization varies within the range of 0-1.
2. Random Range: 0.5-1, Snapshot Interval: Varies, Number of Devices: Varies
   - Energy Efficiency, Response Time, and Throughput have upper limits at 1, but Throughput has a lower limit at 0.5.
   - Resource Utilization ranges between 0 and 1, with values generally higher than in the previous range.
3. Random Range: 0.8-1, Snapshot Interval: Varies, Number of Devices: Varies
   - Energy Efficiency, Response Time, and Throughput have upper limits at 1, and Throughput has a lower limit at 0.8.
   - Resource Utilization is consistently higher, with values primarily between 0.8 and 1.

Based on the data analysis, we can conclude that there is a correlation between Improving Throughput and higher Resource Utilization in the context of the provided dataset. As Throughput improves, Resource Utilization tends to increase as well, especially when the Throughput lower limit is higher (0.5 or 0.8). This suggests that efforts to enhance system throughput may lead to increased utilization of resources. This observation aligns with the nature of resource allocation in systems. When the system aims to process more tasks or requests concurrently to improve throughput, it often requires more resource utilization to accommodate the increased workload.

The similarity in response time and resource utilization with an increasing number of devices in simulation results could be due to various factors and system characteristics. While there is no clear trend, it's essential to consider the potential reasons behind this behavior. A few factors are addressed:

1. Optimization Algorithm Adaptations: my simulation framework incorporates multi-objective optimization algorithms (e.g., NSGA-II and SPEA2) to manage the system's performance. These algorithms are inherently designed to balance response time and resource utilization, especially in the context of fog computing where real-time data processing is crucial. As the number of devices increases, the optimization algorithms adapt to maintain this balance, resulting in relatively stable response times and resource utilization.

2. Resource Scaling: In real-world fog computing scenarios, additional resources (e.g., fog nodes) might be dynamically allocated or scaled up to accommodate a larger number of devices. This scaling process can help in maintaining consistent response times and resource utilization levels despite increased device count.

3. Resource Pooling: Fog computing environments often rely on resource pooling and sharing among devices. As more devices are added, the resource pooling mechanism efficiently allocates resources to ensure that response times are not severely impacted, and resource utilization remains balanced.

4. System Design: The architecture of my telehealth IoT fog computing model is inherently designed to handle scalability efficiently. It employs load balancing techniques, task prioritization, or resource allocation strategies that prevent response time degradation and resource contention, even with an increasing number of devices.

5. Experimental Variability: In some cases, the observed stability in response time and resource utilization are due to the specific dataset or experimental condi-

tions used in my simulation. Real-world scenarios might exhibit more variability, but my simulation setup may not capture all the nuances.

3.6 Discussion

The comprehensive data analysis of various scenarios involving Energy Efficiency, Response Time, Throughput, and Resource Utilization in the context of different parameter configurations provides valuable insights into the trade-offs and interdependencies among these key performance metrics. The findings shed light on how changes in one metric can impact others, offering guidance for optimizing system behavior in Telehealth IoT deployments. The data analysis reveals distinct trade-offs between Energy Efficiency, Response Time, Throughput, and Resource Utilization. As we examine different scenarios, it's evident that there is no one-size-fits-all solution; instead, the optimal balance depends on the specific objectives and constraints of the deployment. Optimizing one metric often comes at the expense of others, highlighting the importance of a holistic approach that considers the interplay between these metrics.

Based on the data analysis, we can conclude that there exists a trade-off between Energy Efficiency, Throughput, Resource Utilization, and Response Time in Telehealth IoT deployments.

- **Impact of Energy Efficiency on Throughput and Resource Utilization:** The results consistently show that increasing Energy Efficiency tends to lead to lower Throughput and resource utilization while increasing Response Time. This relationship indicates that, in the pursuit of energy savings, the system may allocate fewer resources to processing tasks, thereby affecting its capacity to handle concurrent requests efficiently. This is a critical consideration for Telehealth IoT deployments, where balancing performance with energy conservation is vital. Striking the right trade-off requires a deep understanding of the deployment context and the specific requirements of the telehealth applications.

- **Throughput-Resource Utilization Correlation:** The analysis further illustrates a correlation between higher Throughput goals and elevated levels of Resource Utilization. When aiming for improved Throughput, the system often needs to utilize resources more intensively to process tasks concurrently. This observation aligns with the fundamental principle of resource allocation, where meeting higher demands typically requires more resource allocation. Decision-makers must weigh the benefits of increased Throughput against the potential resource strain and its implications on overall system performance.

The findings emphasize the critical role of system design and configuration in achieving desired performance outcomes. Designers and decision-makers should carefully evaluate trade-offs and align system behavior with the specific objectives of their Telehealth IoT deployments. This analysis equips them with the necessary insights to make informed decisions, such as selecting appropriate snapshot intervals and adjusting resource allocation strategies.

In Telehealth IoT deployments, the findings have practical implications for real-world applications. Decision-makers can leverage the analysis to tailor system configurations based on the priorities of their telehealth services. For instance, when minimizing Response Time is crucial, configurations that prioritize lower Response Time while maintaining acceptable levels of other metrics can be chosen. Additionally, solutions with favorable Resource Utilization can be adopted to ensure efficient use of resources while meeting performance targets.

The practical implications of Pareto-optimal solutions are significant for decision-makers involved in Telehealth IoT deployments. These solutions offer a range of trade-off options, allowing decision-makers to customize system configurations based on the specific requirements of their applications. The data analysis has illuminated various scenarios where trade-offs are most apparent. For instance,

- Resource Allocation: Decision-makers can select solutions that strike an optimal balance between Energy Efficiency and Throughput. Depending on the deployment context, they can adjust the allocation of resources to achieve the desired trade-offs.

- Real-time Applications: For telehealth applications that demand low Response Time, decision-makers can identify solutions that minimize Response Time while maintaining acceptable levels of other metrics.

- Resource Efficiency: Solutions with favorable Resource Utilization can be chosen to ensure efficient use of resources while meeting performance targets.

Additionally, the insights provided by Pareto-optimal solutions enable decision-makers to make well-informed choices that align with their strategic goals, ensuring efficient resource utilization while meeting performance targets. Therefore, the

Pareto-optimal solutions have significant practical implications for decision-makers involved in Telehealth IoT deployments. These solutions provide decision-makers with a menu of trade-off options, allowing them to tailor system configurations to meet specific application requirements and priorities.

The data analysis results provide a foundation for understanding the intricate relationships between Energy Efficiency, Response Time, Throughput, and Resource Utilization in Telehealth IoT deployments. The findings underscore the importance of holistic optimization approaches that consider the interdependence among these metrics. By embracing a nuanced understanding of the trade-offs, decision-makers can design and configure systems that strike the right balance between performance, energy efficiency, and resource utilization, ultimately contributing to robust and effective Telehealth IoT deployments. By providing a range of options, Pareto-optimal solutions empower decision-makers to make well-informed choices that align with their strategic goals. This approach facilitates flexible decision-making and encourages a nuanced understanding of the complex relationships between performance metrics, leading to more robust and effective Telehealth IoT deployments.

3.7 Summary

This research serves as a natural progression of our earlier work, which predominantly examined energy efficiency within a fog computing framework. The multi-objective optimization approach plays a pivotal role in enhancing the balance between conflicting performance metrics in Telehealth IoT deployments. Traditionally, focusing on a single objective could lead to suboptimal solutions, as it neglects the impact of changes on other metrics. The analysis shows that optimizing one metric often leads to trade-offs with others, highlighting the complexity of these relationships. The multi-objective optimization framework enables us to identify the Pareto-optimal solutions – those where no single metric can be improved without sacrificing another. By broadening our scope to encompass the multi-objective optimization landscape, we aim to elevate our understanding of how the hybrid fog/cloud computing platform can harmonize the competing demands of energy savings and overall system performance. This research paper makes several significant contributions to the field of Telehealth Internet-of-Things (IoT) fog computing. The study focused on achieving balanced and optimized performance in Telehealth IoT deployments by leveraging the power of multi-objective optimization. By evaluating and analyzing key performance metrics such as Energy Efficiency, Response Time, Throughput, and Resource Utilization, we have uncovered valuable insights that shed light on the intricate trade-offs involved in designing and deploying efficient and effective Telehealth IoT systems. One of the primary contributions of this research lies in the adoption of a multi-objective optimization approach. Unlike traditional single-objective optimization, which often leads to suboptimal outcomes by prioritizing a single metric, our approach considers the interplay of multiple conflicting metrics. This has enabled us to identify a range of Pareto-optimal solutions that strike a harmonious balance between Energy Efficiency, Response Time, Throughput, and Resource Utilization. The significance of incorporating multi-objective optimization in Telehealth IoT fog computing cannot be overstated, as it enhances the decision-making process by providing decision-makers with a comprehensive set of feasible options that cater to different priorities and constraints. Furthermore, the findings of this chapter have a profound impact on optimizing real-world Telehealth IoT systems. The Pareto-optimal solutions offer practical guidance for designing, deploying, and managing Telehealth IoT environments. Decision-makers can leverage these solutions to tailor their system configurations based on specific application requirements and strategic objectives. The potential benefits span a wide spectrum, from resource-efficient allocation to meeting stringent real-time application demands. By optimizing the performance of Telehealth IoT systems, the research paves the way for enhanced patient care, improved operational efficiency, and the potential for transformative advancements in healthcare services. In essence, this chapter underscores the critical role of multi-objective optimization in achieving balanced and optimized performance in Telehealth IoT fog computing. The insights gained through this study provide a valuable roadmap for decision-makers, researchers, and practitioners to navigate the complexities of Telehealth IoT deployments, making a lasting impact on the future of healthcare technology and service delivery.

Chapter 4

Conclusions and Future Directions

4.1 Summary and Conclusions

This dissertation has been dedicated to addressing the critical challenges in telehealth systems through the integration of IoT, fog, and cloud computing. The escalating demand for efficient, real-time data processing and energy conservation in telehealth, driven by the proliferation of IoT devices, has been the focal point of our research.

We introduced an energy-efficient model in Chapter two that combines the low-latency benefits of fog computing with the scalable resources of cloud computing. By processing data locally at fog nodes, the model reduces the need for continuous communication with cloud servers, thereby minimizing energy consumption, latency, and optimizing computational resource utilization. The hybrid offloading model, load prediction algorithm, resource scaling scheme, and energy-efficient data migration techniques developed in this research have been validated through comprehensive simulation studies. These studies demonstrated significant reductions in energy consumption while maintaining high levels of scalability and responsiveness, compared to traditional cloud-only architectures.

In the simulation studies, we deliberately limited the number of devices and network conditions. This approach was strategic and necessary for several reasons. First, it allowed us to create controlled environments where we could isolate and understand the impact of specific variables on the performance of our model. For instance, by varying the number of devices from 10 to 1000, we could observe how the model scaled and how energy consumption, latency, and other performance metrics were affected. Limiting the network conditions enabled us to test the model's resilience and efficiency under different levels of stress. Moreover, in real-world scenarios, it is often the case that telehealth deployments start small and gradually expand. Our simulations, with a limited number of devices, can accurately represent these initial deployment phases. The results obtained from these simulations provide a solid foundation for understanding the model's behavior and predicting its performance as the scale increases. Despite the limitations in simulation parameters, the consistent trends and significant differences observed in energy consumption, latency, and other metrics between our proposed model and traditional architectures validate the effectiveness and meaningfulness of our research. The model's ability to outperform traditional approaches in these controlled simulations strongly suggests its potential for real-world applications.

The multi-objective optimization approach in chapter three further enhanced our understanding of the complex trade-offs between energy efficiency, response time, throughput, and resource utilization. By identifying Pareto-optimal solutions, we provided decision-makers with valuable insights into tailoring system configurations based on specific application requirements.

4.2 Future Directions

4.2.1 Advanced Optimization Algorithms

Future research should focus on developing more sophisticated optimization algorithms. Hybrid algorithms that combine the strengths of existing algorithms like NSGA-II and SPEA2 could be explored. These hybrid algorithms could potentially offer better convergence and diversity, leading to more optimal solutions. Additionally, adaptive objective weighting schemes could be developed to dynamically adjust the significance of objectives based on system states or user preferences. This would provide more flexibility in optimizing the system for different scenarios.

4.2.2 Real-world Validation

To further validate the practicality of our model, real-world deployments and pilot studies are essential. By implementing the model in actual telehealth settings, we can gather real data on its performance, user acceptance, and potential barriers to implementation. Comparing the real-world results with the simulation outcomes will help refine the model and ensure its applicability in diverse healthcare environments.

4.2.3 Integration of Emerging Technologies

The integration of emerging technologies such as artificial intelligence and machine learning holds great promise. These technologies can be used to enhance data analytics capabilities, enabling more accurate diagnostics and personalized treatment plans. For example, machine learning algorithms can be applied to analyze the vast amounts of healthcare data processed by the system, identifying patterns and making predictions to improve patient care.

4.2.4 Security and Privacy Enhancements

As telehealth systems handle sensitive patient data, enhancing security and privacy is of utmost importance. Future research should focus on developing advanced security measures and privacy-preserving techniques for telehealth IoT devices and fog nodes. This includes exploring encryption techniques, access control mechanisms, and secure data transmission protocols to ensure the protection of patient information.

4.2.5 Interoperability and Standardization

To facilitate seamless communication and integration across different healthcare systems, solutions that promote interoperability and standardization should be explored. This involves developing common protocols and standards for telehealth IoT devices, fog nodes, and cloud platforms, enabling them to work together more effectively.

In conclusion, this research has made significant contributions to the field of telehealth by proposing an energy-efficient model and exploring multi-objective optimization techniques. The future research directions outlined here will further enhance the capabilities of telehealth systems, leading to more sustainable, efficient, and effective healthcare services.

4.2.6 Contributions

This research resulted in the following publications:

1. Guo, Y., Sudhakar. G., Wu, Y. (2024). Enhancing Energy Efficiency in Telehealth Internet-of-Things Systems Through Fog and Cloud Computing Inte-

gration: Simulation Study. JMIR Biomed Eng. PMID: 38875671 PMCID: PMC11041449 DOI: 10.2196/50175

2. Guo. Y., Sudhakar. G. and Guo. B (2024) " An Energy-Efficient Model of Integrating Telehealth IoT Devices with Fog and Cloud Computing-Based Platform" World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering. Vol:18, No:4.

3. Guo. Y., Sudhakar. G. Guo. B. and Guo. N. (2024) "Enhancing Energy Efficiency in Telehealth IoT through Multi-Objective Optimization on a Hybrid Fog/Cloud Computing Platform" Journal of Biotechnology & Bioinformatics Research. ISSN: 2755-0168; Volume 6(3):1-12

4. Guo. Y., Sudhakar. G. and Guo. B (2024) "Enhancing Energy Efficiency in Telehealth IoT Through Multi-Objective Optimization" IEEE, ISSN: 2769-4542, DOI: 10.1109/ICICT62343.2024.00072

Bibliography

[1] Ranesh Kumar Naha, Saurabh Garg, and Andrew Chan. *Fog-computing architecture: survey and challenges*, page 199–223. Institution of Engineering and Technology, November 2019.

[2] Luis M Vaquero, Luis Rodero-Merino, Juan Caceres, and Maik Lindner. A break in the clouds: towards a cloud definition, 2008.

[3] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *2008 10th IEEE international conference on high performance computing and communications*, pages 5–13. Ieee, 2008.

[4] O. Shimrat. Cloud computing and healthcare. Available online: `http://www.himss.org/content/files/Code%2093_Shimrat_CloudComputingandHealthcare_2009.pdf` (accessed on 2 February 2021), 2009.

[5] P Mell. The nist definition of cloud computing. *Recommendations of the National Institute of Standards and Technology*, 2011.

[6] Daniele Catteddu. Cloud computing: benefits, risks and recommendations for information security. In *Web Application Security: Iberic Web Application Security Conference, IBWAS 2009, Madrid, Spain, December 10-11, 2009. Revised Selected Papers*, pages 17–17. Springer, 2010.

[7] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 85–90, 2009.

[8] Lutz Schubert, Keith Jeffery, Burkhard Neidecker-Lutz, Prashant Barot, Francis Behr, Peter Bosch, and Ivona Brandic. The future of cloud computing-opportunities for european cloud computing beyond 2010. 2010.

[9] J Haughton. Year of the underdog: Cloud-based ehrs. *Health Manag Technol*, 32(1):9, 2011.

[10] Chia-Chi Teng, Jonathan Mitchell, Christopher Walker, Alex Swan, Cesar Davila, David Howard, and Travis Needham. A medical image archive solution in the cloud. In *2010 IEEE International Conference on Software Engineering and Service Sciences*, pages 431–434. IEEE, 2010.

[11] Cloud computing in healthcare: 9 benefits of cloud computing. Available online: `https://symphony-solutions.com/insights/benefits-of-cloud-computing-in-healthcare` (accessed on February 5, 2021), 2013.

[12] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[13] Lejiang Guo, Fangxin Chen, Li Chen, and Xiao Tang. The building of cloud computing environment for e-health. In *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, volume 1, pages 89–92. IEEE, 2010.

[14] Peter G Goldschmidt. Hit and mis: implications of health information technology and medical information systems. *Communications of the ACM*, 48(10):68–74, 2005.

[15] Elizabeth Davidson and Dan Heslinga. Bridging the it adoption gap for small physician practices: An action research study on electronic health records. *Information Systems Management*, 24(1):15–28, 2006.

[16] Richard Klein. An empirical examination of patient-physician portal acceptance. *European Journal of Information Systems*, 16(6):751–760, 2007.

[17] Richard Lenz and Manfred Reichert. It support for healthcare processes–premises, challenges, perspectives. *Data & Knowledge Engineering*, 61(1):39–58, 2007.

[18] European Commission. Protecting your personal data. Available online: `http://ec.europa.eu/justice/data-protection/individuals/index_en.htm` (accessed on February 21, 2021), 2013.

[19] James M DuBois, Jessica Mozersky, Meredith Parsons, Heidi A Walsh, Annie Friedrich, and Amy Pienta. Exchanging words: Engaging the challenges of sharing qualitative research data. *Proceedings of the National Academy of Sciences*, 120(43):e2206981120, 2023.

[20] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[21] Shreyas Sen. Context-aware energy-efficient communication for iot sensor nodes. In *Proceedings of the 53rd Annual Design Automation Conference*, pages 1–6, 2016.

[22] Davide Calvaresi, Daniel Cesarini, Paolo Sernani, Mauro Marinoni, Aldo Franco Dragoni, and Arnon Sturm. Exploring the ambient assisted living domain: a systematic review. *Journal of Ambient Intelligence and Humanized Computing*, 8:239–257, 2017.

[23] Higinio Mora, Virgilio Gilart-Iglesias, Raquel Pérez-del Hoyo, and María Dolores Andújar-Montoya. A comprehensive system for monitoring urban accessibility in smart cities. *Sensors*, 17(8):1834, 2017.

[24] Kyunghee Sun and Intae Ryoo. A smart sensor data transmission technique for logistics and intelligent transportation systems. In *Informatics*, volume 5, page 15. MDPI, 2018.

[25] Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, and Siobhán Clarke. Middleware for internet of things: a survey. *IEEE Internet of things journal*, 3(1):70–95, 2015.

[26] Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, and Amit P Sheth. Machine

learning for internet of things data analysis: A survey. *Digital Communications and Networks*, 4(3):161–175, 2018.

[27] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. In *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*, pages 46–51. Ieee, 2007.

[28] Mu-Sheng Lin, Jenq-Shiou Leu, Kuen-Han Li, and Jean-Lien C Wu. Zigbee-based internet of things in 3d terrains. *Computers & Electrical Engineering*, 39(6):1667–1683, 2013.

[29] Il-Gu Lee and Myungchul Kim. Interference-aware self-optimizing wi-fi for high efficiency internet of things in dense networks. *Computer Communications*, 89:60–74, 2016.

[30] Dan Chen, Zhixin Liu, Lizhe Wang, Minggang Dou, Jingying Chen, and Hui Li. Natural disaster monitoring with wireless sensor networks: A case study of data-intensive applications upon low-cost scalable systems. *Mobile Networks and Applications*, 18:651–663, 2013.

[31] Karen Rose, Scott Eldridge, and Lyman Chapin. The internet of things: An overview. *The internet society (ISOC)*, 80(15):1–53, 2015.

[32] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[33] Dieter Uckelmann, Mark Harrison, and Florian Michahelles. An architectural approach towards the future internet of things. In *Architecting the internet of things*, pages 1–24. Springer, 2011.

[34] Salvatore Distefano, Dario Bruneo, Francesco Longo, Giovanni Merlino, and Antonio Puliafito. Hospitalized patient monitoring and early treatment using iot and cloud. *BioNanoScience*, 7:382–385, 2017.

[35] Louise E Moser and PM Melliar-Smith. Personal health monitoring using a smartphone. In *2015 IEEE International Conference on Mobile Services*, pages 344–351. IEEE, 2015.

[36] Antonio J Jara, Miguel A Zamora-Izquierdo, and Antonio F Skarmeta. Interconnection framework for mhealth and remote monitoring based on the internet of things. *IEEE Journal on Selected Areas in Communications*, 31(9):47–65, 2013.

[37] Jeong-Yong Byun, Aziz Nasridinov, and Young-Ho Park. Internet of things for smart crime detection. *Contemporary Engineering Sciences*, 7(15):749–754, 2014.

[38] Sanaz Rahimi Moosavi, Amir-Mohammad Rahmani, Tomi Westerlund, Geng Yang, Pasi Liljeberg, Hannu Tenhunen, et al. Pervasive health monitoring based on internet of things: Two case studies. In *2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, pages 275–278. IEEE, 2014.

[39] Vandana Milind Rohokale, Neeli Rashmi Prasad, and Ramjee Prasad. A cooperative internet of things (iot) for rural healthcare monitoring and control. In *2011 2nd international conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE)*, pages 1–6. IEEE, 2011.

[40] Jakob Branger and Zhibo Pang. From automated home to sustainable, healthy and manufacturing home: a new story enabled by the internet-of-things and industry 4.0. *Journal of Management Analytics*, 2(4):314–332, 2015.

[41] Hemant Ghayvat, Subhas Mukhopadhyay, Xiang Gui, and Nagender Suryadevara. Wsn-and iot-based smart homes and their extension to smart buildings. *sensors*, 15(5):10350–10379, 2015.

[42] Ilias Maglogiannis, Margrit Betke, Grammati Pantziou, and Fillia Makedon. Assistive environments for the disabled and the senior citizens: theme issue of petra 2010 and 2011 conferences, 2014.

[43] K Divya Krishna, Vivek Akkala, Ramkrishna Bharath, Pachamuthu Rajalakshmi, and Abdul Mateen Mohammed. Fpga based preliminary cad for kidney on iot enabled portable ultrasound imaging system. In *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 257–261. IEEE, 2014.

[44] Boyi Xu, Li Da Xu, Hongming Cai, Cheng Xie, Jingyuan Hu, and Fenglin Bu. Ubiquitous data accessing method in iot-based information system for emergency medical services. *IEEE Transactions on Industrial informatics*, 10(2):1578–1586, 2014.

[45] Rajesh Vargheese and Yannis Viniotis. Influencing data availability in iot enabled cloud based e-health in a 30 day readmission context. In *10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 475–480. IEEE, 2014.

[46] Iman Azimi, Amir M Rahmani, Pasi Liljeberg, and Hannu Tenhunen. Internet of things for remote elderly monitoring: a study from user-centered perspective. *Journal of ambient intelligence and humanized computing*, 8:273–289, 2017.

[47] Feifei Shi, Qingjuan Li, Tao Zhu, and Huansheng Ning. A survey of data semantization in internet of things. *Sensors*, 18(1):313, 2018.

[48] Moonmoon Chakraborty. Fog computing vs. cloud computing. *arXiv preprint arXiv:1904.04026*, 2019.

[49] Ganjar Alfian, Muhammad Syafrudin, Muhammad Fazal Ijaz, M Alex Syaekhoni, Norma Latif Fitriyani, and Jongtae Rhee. A personalized healthcare monitoring system for diabetic patients by utilizing ble-based sensors and real-time data processing. *Sensors*, 18(7):2183, 2018.

[50] Sujata Dash, Sitanath Biswas, Debajit Banerjee, and Atta UR Rahman. Edge and fog computing in healthcare–a review. *Scalable Computing: Practice and Experience*, 20(2):191–206, 2019.

[51] Shreshth Tuli, Nipam Basumatary, Sukhpal Singh Gill, Mohsen Kahani, Rajesh Chand Arya, Gurpreet Singh Wander, and Rajkumar Buyya. Healthfog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated iot and fog computing environments. *Future Generation Computer Systems*, 104:187–200, 2020.

[52] Aparna Kumari, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. Fog computing for healthcare 4.0 environment: Opportunities and challenges. *Computers & Electrical Engineering*, 72:1–13, 2018.

[53] Hany F Atlam, Robert J Walters, and Gary B Wills. Fog computing and the internet of things: A review. *big data and cognitive computing*, 2(2):10, 2018.

[54] Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt, and Behnam Zakeri. Internet of things (iot) and the energy sector. *Energies*, 13(2):494, 2020.

[55] Richard Wootton. Telemedicine. *British Journal of Hospital Medicine*, 73(9):504–507, 2012.

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

[57] P Kumar, K Patil, JH Lee, and HJ Lee. Iot-based remote patient monitoring: a survey on the capabilities, challenges, and future directions. *Electronics*, 9(10):1702, 2020.

[58] Bruno MC Silva, Joel JPC Rodrigues, Isabel de la Torre Díez, Miguel López-Coronado, and Kashif Saleem. Mobile-health: A review of current state in 2015. *Journal of biomedical informatics*, 56:265–272, 2015.

[59] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16, 2012.

[60] Shanhe Yi, Cheng Li, and Qun Li. A survey of fog computing: concepts, applications and issues. In *Proceedings of the 2015 workshop on mobile big data*, pages 37–42, 2015.

[61] Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, and Eui-Nam Huh. Cloud of things: Integrating internet of things and cloud computing and the issues involved. In *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*, pages 414–419. IEEE, 2014.

[62] Harishchandra Dubey, Jing Yang, Nick Constant, Amir Mohammad Amiri, Qing Yang, and Kunal Makodiya. Fog data: Enhancing telehealth big data through fog computing. In *Proceedings of the ASE bigdata & socialinformatics 2015*, pages 1–6. 2015.

[63] Olena Skarlat, Stefan Schulte, Michael Borkowski, and Philipp Leitner. Resource provisioning for iot services in the fog. In *2016 IEEE 9th international conference on service-oriented computing and applications (SOCA)*, pages 32–39. IEEE, 2016.

[64] Mu-Hsing Kuo et al. Opportunities and challenges of cloud computing to improve health care services. *Journal of medical Internet research*, 13(3):e1867, 2011.

[65] Joel JPC Rodrigues, Isabel de la Torre, Gonzalo Fernández, and Miguel López-Coronado. Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of medical Internet research*, 15(8):e186, 2013.

[66] M. Hussain, F. Chen, and A. Ali. Cloud-based telehealth system for integrated services in smart cities. *IEEE Communications Magazine*, 53(12):68–73, 2015.

[67] Fatemeh Jalali, Kerry Hinton, Robert Ayre, Tansu Alpcan, and Rodney S Tucker. Fog computing may help to save energy in cloud computing. *IEEE Journal on Selected Areas in Communications*, 34(5):1728–1739, 2016.

[68] G. Orsini, D. Bade, and W. Lamersdorf. Computing in the fog: A real-world iot architecture for smart cities. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[69] Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, and Wei Ni. Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, 21(2):1636–1675, 2018.

[70] Zaheer Khan, Zeeshan Pervez, and Abdul Ghafoor. Towards cloud based smart cities data security and privacy management. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pages 806–811. IEEE, 2014.

[71] U. Gormus, A. Kansal, and M. B. Srivastava. Energy-aware lossless data compression. *ACM Transactions on Sensor Networks (TOSN)*, 7(3):1–25, 2011.

[72] Mung Chiang and Tao Zhang. Fog and iot: An overview of research opportunities. *IEEE Internet of things journal*, 3(6):854–864, 2016.

[73] Subhadeep Sarkar, Subarna Chatterjee, and Sudip Misra. Assessment of the suitability of fog computing in the context of internet of things. *IEEE Transactions on Cloud Computing*, 6(1):46–59, 2015.

[74] M. Abdel-Basset, V. Chang, and H. Hawash. A fusion of cloud-fog based smart city model for efficient performance. *Computers, Materials Continua*, 57(3):337–355, 2019.

[75] Roberto Morabito. Virtualization on internet of things edge devices with container technologies: A performance evaluation. *IEEE Access*, 5:8835–8850, 2017.

[76] S. Tuli, S. Singh Gill, R. C. Arya, M. Shojafar, and R. Buyya. Fogbus: A lightweight and qos-aware framework for the internet of things. *IEEE Internet of Things Journal*, 7(5):4493–4510, 2020.

[77] Harshit Gupta, Amir Vahid Dastjerdi, Soumya K Ghosh, and Rajkumar Buyya. ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. *Software: Practice and Experience*, 47(9):1275–1296, 2017.

[78] Jessica Oueis, Emilio Calvanese Strinati, and Sergio Barbarossa. The fog balancing: Load distribution for small cell cloud computing. In *2015 IEEE 81st vehicular technology conference (VTC spring)*, pages 1–6. IEEE, 2015.

[79] Marc Barcelo, Alejandro Correa, Jaime Llorca, Antonia M Tulino, Jose Lopez Vicario, and Antoni Morell. Iot-cloud service optimization in next generation smart environments. *IEEE Journal on Selected Areas in Communications*, 34(12):4077–4090, 2016.

[80] X Zeng, S Garg, and P Strazdins. A comparative study of iot cloud and fog computing simulations using ifogsim and cooja. In *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)*, pages 108–113, 2017.

[81] Charles C Byers and Patrick Wetterwald. Fog computing distributing data and intelligence for resiliency and scale necessary for iot: The internet of things (ubiquity symposium). *Ubiquity*, 2015(November):1–12, 2015.

[82] PJ Bermejo, S Rodríguez, DR Valladares, and J Boubeta-Puig. Yafs: a simulator for iot scenarios in fog computing. *IEEE Access*, 8:111908–111922, 2020.

[83] AM García, JP Pérez, and OJ Bellido. Yafs: a simulator for iot scenarios in fog computing. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 215–222, 2018.

[84] Yunyong Guo, Sudhakar Ganti, Yi Wu, et al. Enhancing energy efficiency in telehealth internet of things systems through fog and cloud computing integration: Simulation study. *JMIR biomedical engineering*, 9(1):e50175, 2024.

[85] Mohammad Aazam and Eui-Nam Huh. Fog computing and smart gateway based communication for cloud of things. In *2014 International conference on future internet of things and cloud*, pages 464–470. IEEE, 2014.

[86] Prabal Verma and Sandeep K Sood. Fog assisted-iot enabled patient health monitoring in smart homes. *IEEE Internet of Things Journal*, 5(3):1789–1796, 2018.

[87] A. Koubaâ, B. Qureshi, M. F. Sriti, A. Allouch, and Y. Javed. A fog-based emergency and healthcare system for smart cities. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[88] S. Sareen, S. K. Sood, and S. K. Gupta. Energy-efficient context-aware framework for managing application execution in cloud-fog environment. *International Journal of Communication Networks and Distributed Systems*, 15(2-3):137–154, 2015.

[89] M. M. Alam, M. B. I. Reaz, M. A. Ashraf, M. S. Hossain, M. T. Islam, and S. Otoum. Telehealth iot devices integrated with fog nodes and private/public cloud architecture model. *IEEE Access*, 7:108636–108647, 2019.

[90] American Heart Association et al. Understanding blood pressure readings, 2017.

[91] Julius Mwaniki. Investigating the impact of exercise intensity on cardiovascular health parameters in kenya. *American Journal of Physical Sciences*, 2(2):24–38, 2024.

[92] American Lung Association. Respiratory rate. Retrieved from `https://www.lung.org/lung-health-diseases/lung-procedures-and-tests/respiratory-rate`, 2018. Accessed: 2021-02-05.

[93] LaTonya S Brailsford. *Engaging Nurses in an Antimicrobial Stewardship Program to Combat Clostridium difficile*. PhD thesis, Grand Canyon University, 2020.

[94] MedlinePlus. Oxygen saturation. Retrieved from `https://medlineplus.gov/oxygenlevels.html`, 2021. Accessed: 2021-02-05.

[95] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, 4(5):1125–1142, 2017.

[96] G. Abdu, H. Wan Hassan, and S. S. Siti. A review of internet of things for smart home: Challenges and solutions. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 2018.

[97] Jean-Paul Viricelle, Arthur Valleron, Christophe Pijolat, Philippe Breuil, and Sébastien Ott. Gas sensors based on tin dioxide for exhaust gas application, modeling of response for pure gases and for mixtures. *Procedia Engineering*, 47:655–658, 2012.

[98] Salvatore J Stolfo, Malek Ben Salem, and Angelos D Keromytis. Fog computing: Mitigating insider data theft attacks in the cloud. In *2012 IEEE symposium on security and privacy workshops*, pages 125–128. IEEE, 2012.

[99] Luce Grosjean. Spotted. In *ACM SIGGRAPH 2014 Computer Animation Festival*, pages 1–1. 2014.

[100] Yunyong Guo, Sudhakar Ganti, and Bryan Guo. Enhancing energy efficiency in telehealth iot through multi-objective optimization. In *2024 7th International Conference on Information and Computer Technologies (ICICT)*, pages 406–412. IEEE, 2024.

[101] Tuan Nguyen Gia, Mingzhe Jiang, Amir-Mohammad Rahmani, Tomi Westerlund, Pasi Liljeberg, and Hannu Tenhunen. Fog computing in healthcare internet of things: A case study on ecg feature extraction. In *2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing*, pages 356–363. IEEE, 2015.

[102] S. Islam, M. Shamim Hossain, and C. Hong. Optimization of iot data processing for healthcare applications in fog computing. *IEEE Access*, 2020.

[103] S. Heo, M. Choi, and J. Cha. Fog computing for healthcare iot: Integration and performance analysis. *Journal of Ambient Intelligence and Humanized Computing*, 2020.

[104] Kalyanmoy Deb, Amrit Pratap, Sameer Agarwal, and TAMT Meyarivan. A fast and elitist multiobjective genetic algorithm: Nsga-ii. *IEEE transactions on evolutionary computation*, 6(2):182–197, 2002.

[105] Marco Laumanns. Spea2: Improving the strength pareto evolutionary algorithm. *Technical Report, Gloriastrasse 35*, 2001.

[106] Q. Qi, L. Zhang, X. Shen, and Y. Huang. Multi-objective optimization with nsga-ii algorithm for space mission design. In *Proceedings of the International Astronautical Congress*, 2016. Accessed on August 15, 2023.

[107] Qiang He, Zhaolin Xi, Zheng Feng, Yueyang Teng, Lianbo Ma, Yuliang Cai, and Keping Yu. Telemedicine monitoring system based on fog/edge computing: A survey. *IEEE Transactions on Services Computing*, 2024.

[108] Kalyanmoy Deb, Karthik Sindhya, and Jussi Hakanen. Multi-objective optimization. In *Decision sciences*, pages 161–200. CRC Press, 2016.

[109] Mahadev Satyanarayanan. The emergence of edge computing. *Computer*, 50(1):30–39, 2017.

[110] S. Kumar and S. S. Gill. Optimization challenges in telehealth iot: A comprehensive review. *Computers in Biology and Medicine*, 124:103958, 2022.

[111] Marco Lombardi, Francesco Pascale, and Domenico Santaniello. Internet of things: A general overview between architectures, protocols and applications. *Information*, 12(2):87, 2021.

[112] S. Raza, L. Wallgren, and T. Voigt. Evaluating the performance of coap-based protocol stacks for the internet of things. *Sensors*, 14(11):18845–18885, 2019.