Interoperability Solution for Internet of Medical Things in Telemedicine

Wasiu Olakayode OLAYINKA
LCU/PG/002846

Being a MSc Thesis Presentation Submitted to the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria

In Partial Fulfilment of the Requirements for the Award of Master of Science Degree (MSc) in Computer Science

2024

Certification

This is to Certify that Wasiu Olakayode OLAYINKA with matriculation number LCU/PG/002846 carried out this research with title "Development of Interoperability Solution for Internet of Medical Things in Telemedicine" in the Department of Computer Science, Faculty of Natural and Applied Science, Lead City University, Ibadan, Oyo state for the award of Master of Science Degree (MSc) in Computer Science and that this has not been previously submitted.

…… ……

Professor S. O. Akinola Date

Supervisor

…… ……

Dr. W. Sakpere Date

Head of Department

Dedication

This research is dedicated to Almighty God for his mercies, guidance, and protection during this program and beyond.

Acknowledgment

I would like to express my deepest gratitude to Professor S. O. Akinola for his exceptional mentorship throughout my MSc program. His invaluable guidance and unwavering support have profoundly shaped both my academic and professional development. I feel truly fortunate to have had the opportunity to learn under his expertise, and I am immensely grateful for the significant role he has played in my journey.

I also extend my heartfelt appreciation to the Head of Department, Dr. W. Sakpere, for his outstanding leadership and tireless efforts in creating a nurturing and innovative academic environment. His vision for the department and commitment to excellence have been truly inspiring. The support, encouragement, and opportunities provided by Dr. W. Sakpere have greatly contributed to my success and growth throughout this program.

Furthermore, I would like to thank Dr. A. Waheed for being a source of strength and encouragement during my studies. His insightful guidance and dedication to fostering a conducive learning environment have been instrumental in my academic achievements, and I am sincerely appreciative of his mentorship.

In addition to these individuals, I wish to acknowledge Lead City University for providing a platform that encourages academic excellence and personal growth. The university's commitment to quality education and its supportive staff have been critical to my progress. I am deeply grateful to the faculty and staff of the Department of Computer Science for their continuous efforts in ensuring a thriving academic experience for all students.

Abstract

This study addresses the critical problem of interoperability in the Internet of Medical Things (IoMT) within telemedicine ecosystems, which stems from the integration of diverse medical devices and inconsistent data types. These challenges often lead to inefficient data exchange, hinder remote patient monitoring, and complicate system integration. To enhance the efficiency and effectiveness of telemedicine, the project proposes an API-based interoperability solution that facilitates seamless communication and data exchange. By acting as a standardized interface between devices, the API ensures compatibility across different medical systems by incorporating communication protocols, security measures, and data models. The study also explores how this API-based approach can improve remote monitoring, patient care, and the integration of healthcare systems. Leveraging IoMT technologies through this solution strengthens telemedicine infrastructure, fostering a more cohesive and integrated healthcare environment.

Keywords: API, Data exchange, Interoperability, Internet of Medical Things (IoMT), Medical devices, Telemedicine.

Word Count: 143 words

Table of Contents

List of Figures

List of Acronyms

Abbreviation	Meaning
IOMT	Internet of Medical Things
IoT	Internet of Things
RFID	Radio Frequency Identification
IP	Internet Protocol
Wi-Fi	Wireless Fidelity
LAN	Local Area Network
WLAN	Wireless Local Area Network
NFC	Near Filed Communication
WSN	Wireless Sensor Networks
API	Application User Interface
AI	Artificial Intelligence
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
IoWDs	Internet of Wearable Devices
IMDs	Implantable Medical Devices
DICOM	Digital Imaging and Communications in Medicine
XML	Extensible Markup Language
HL7	Health Level Seven
HER	Electronic Health Record Formats

IDS Intrusion Detection Systems

Appendices

Chapter One

Introduction

1.1 Background to the Study

The integration of the Internet of Medical Things (IoMT) with telemedicine is transforming healthcare, especially in the wake of recent technological advancements and the COVID-19 pandemic. Telemedicine, the remote provision of healthcare through telecommunications, has seen accelerated adoption due to the need for safe, contactless healthcare during global health crises [1]. IoMT, a subset of the Internet of Things (IoT) specific to healthcare, encompasses networked medical devices, sensors, and software that continuously monitor and transmit health data. Together, these technologies enable remote patient monitoring, enhanced diagnostics, and personalized care, marking a significant step toward the modernization of healthcare systems[2].

IoMT in telemedicine creates unique opportunities for healthcare systems to expand access to medical services, particularly for patients in remote or underserved regions. The potential of this integration lies in real-time health data collection, which can enhance clinical decision-making and patient outcomes. As IoMT devices collect and transmit various physiological metrics, they allow healthcare providers to monitor vital signs, detect early warning signs of disease, and tailor treatments based on continuous data feedback[3]. This proactive and data-driven approach represents a shift from traditional reactive healthcare to preventive and personalized medicine, a shift that aligns with broader trends in digital health[4].

However, despite its potential, the integration of IoMT with telemedicine platforms poses significant challenges, especially in terms of interoperability, data privacy, and security. These issues are becoming increasingly critical as IoMT adoption grows. Interoperability—the

seamless communication and data exchange between devices and platforms from different manufacturers—remains one of the primary obstacles to efficient IoMT deployment in telemedicine. Without standardized communication protocols, healthcare providers struggle to integrate IoMT data into electronic health records (EHRs), limiting the usefulness of this data in clinical decision-making[4].

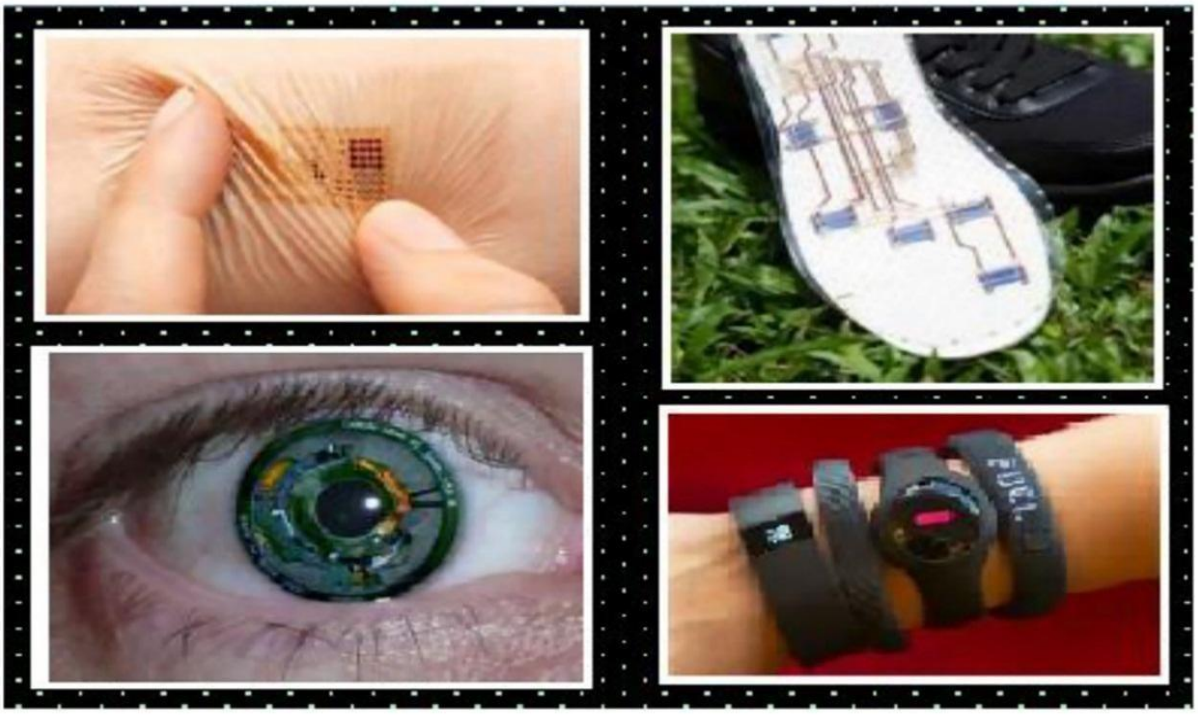


Figure 1.1:Shows various IoMT Devices[7]

Figure 1.1 exemplifies the diversity within IoMT. Devices such as wearable patches, smart insoles, and smart contact lenses demonstrate how various sensors and data-gathering devices can facilitate personalized care. For example:

- **Wearable Patches** continuously monitor parameters like heart rate and temperature, essential for patients with chronic conditions.

- **Smart Insoles** assist in tracking mobility and are valuable in geriatric care.
- **Smart Contact Lenses** help monitor intraocular pressure, aiding in the management of conditions like glaucoma[5].

These devices emphasize the scope of IoMT in healthcare and underscore the importance of interoperability in enabling these diverse devices to function within a unified telemedicine framework.

1.1.1 The Importance of IoMT in Telemedicine

IoMT plays a crucial role in telemedicine by enabling remote, continuous health monitoring. This capability is especially valuable in managing chronic diseases such as diabetes, hypertension, and heart disease, where ongoing monitoring is essential to manage and mitigate health risks. For example, continuous glucose monitoring (CGM) devices transmit real-time data on blood sugar levels to healthcare providers, allowing them to make timely adjustments to treatment plans[6]. Real-time health data facilitates timely interventions, which can improve patient outcomes and reduce the likelihood of complications[7].

The COVID-19 pandemic accelerated the adoption of IoMT and telemedicine as healthcare systems worldwide sought contactless ways to manage patients. IoMT-enabled devices allowed healthcare providers to monitor patients without physical interaction, reducing the risk of infection for both patients and providers. This period underscored the potential of IoMT and telemedicine in creating resilient healthcare systems capable of handling high patient volumes during public health emergencies[8]. Despite this rapid adoption, challenges such as data security, regulatory compliance, and interoperability persist, making it essential to develop solutions that address these issues to sustain and expand the use of IoMT in telemedicine[9].

1.1.2 Challenges in IoMT Integration with Telemedicine

1. **Interoperability**: The diversity of IoMT devices poses a challenge for data integration. Each device may use different communication protocols, data formats, and interfaces, hindering seamless data exchange and integration with telemedicine platforms. Without standardized interoperability solutions, healthcare providers face difficulties in consolidating data from multiple IoMT devices into a coherent patient record, limiting the effectiveness of telemedicine services[9].

Efforts to standardize protocols, such as the development of the Fast Healthcare Interoperability Resources (FHIR) standard by HL7, aim to address these interoperability issues. FHIR provides a framework for integrating different healthcare systems by establishing data formats and elements, allowing IoMT devices to communicate with various telemedicine platforms more effectively[10]. Nevertheless, widespread adoption of these standards across IoMT manufacturers remains limited, creating barriers to seamless healthcare delivery.

2. **Data Security and Privacy**: IoMT devices collect vast amounts of sensitive health data, raising concerns about data security and patient privacy. Data breaches or unauthorized access to health information can compromise patient confidentiality and trust in telemedicine services. Securing IoMT data requires robust encryption and compliance with healthcare regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA)[11].

Recent studies highlight the increasing sophistication of cyber threats targeting IoMT systems. Attackers can exploit vulnerabilities in device firmware or network protocols to gain access to health data. Addressing these threats involves implementing end-to-end encryption, multi-factor authentication, and regular software updates, which are essential for safeguarding patient data in telemedicine applications[12].

3. **Power Efficiency and Device Longevity**: Many IoMT devices, particularly wearables and implantable, have limited battery life. This limitation restricts continuous monitoring and may interrupt data collection, compromising patient care. Researchers are exploring energy-efficient communication protocols, such as Bluetooth Low Energy (BLE), and power optimization techniques to enhance the longevity of IoMT devices, thus supporting reliable, uninterrupted monitoring[13].

1.1.3 Evolution of Healthcare Models with IoMT

The integration of IoMT into healthcare reflects a shift from traditional in-person care to a more proactive, data-driven approach. Traditional healthcare delivery relied on scheduled visits and patient self-reporting, leading to delayed responses to emerging health issues. In contrast, IoMT enables continuous data collection, which provides healthcare providers with a real-time view of a patient's health status. This evolution from episodic to continuous care allows for early intervention, which is particularly beneficial in managing chronic conditions that require frequent monitoring and timely adjustments to treatment[14].

Moreover, IoMT devices are increasingly integrated with AI-powered analytics that interpret health data and assist in clinical decision-making. For instance, AI algorithms can analyse patterns in data from wearable ECG monitors to detect arrhythmias, prompting providers to investigate potential heart issues before symptoms worsen[15]. This combination of IoMT and AI enhances telemedicine by allowing for predictive and preventive healthcare, where insights from continuous monitoring inform personalized care strategies.

1.1.4 Technological Components of IoMT

1. **Wearable and Implantable Devices**: IoMT consists of various types of devices, including wearable and implantable sensors, that gather health data. Examples include wearable fitness trackers, ECG

monitors, and glucose monitors. Implantable devices, like pacemakers and insulin pumps, offer critical health management functions for specific conditions[19].

2. **Data Transmission Technologies**: Reliable data transmission is essential in IoMT, with devices commonly using Bluetooth, Wi-Fi, and cellular networks. Some systems employ gateways to aggregate data from multiple devices, ensuring seamless and secure transmission to telemedicine platforms or cloud storage[5].

3. **Data Storage and Analytics**: The volume of data generated by IoMT devices requires significant storage and analytics capabilities. Cloud platforms provide scalable storage solutions, while advanced analytics and machine learning algorithms interpret data, offering actionable insights for healthcare providers.

1.1.5 Benefits and Future Prospects of IoMT in Healthcare

The integration of IoMT in telemedicine offers numerous benefits, including:

- **Improved Access to Care**: IoMT enhances healthcare accessibility by enabling remote monitoring, which is especially beneficial for patients in rural or underserved areas.
- **Patient Empowerment**: Patients gain access to their health data through connected devices, empowering them to participate actively in their own healthcare[3].
- **Enhanced Efficiency**: IoMT reduces the frequency of in-person visits and optimizes healthcare resource allocation, creating a more efficient and patient-cantered healthcare system[25].

As IoMT technology continues to evolve, addressing interoperability and security challenges will be crucial. Developing standardized communication protocols and ensuring data protection will enhance the reliability and acceptance of IoMT in telemedicine. Future research will focus on

refining these technologies and exploring new applications in preventive care, diagnostics, and chronic disease management, driving further innovations in healthcare delivery[12].

1.2 Statement of the Problem

The COVID-19 pandemic has underscored the urgent need for remote healthcare solutions, highlighting the limitations of traditional healthcare systems. Patients delaying or avoiding medical treatments emphasized the importance of real-time access to healthcare through remote monitoring and consultations. The Internet of Medical Things (IoMT) offers a promising solution by integrating interconnected medical devices, sensors, and applications that can collect and transmit crucial patient data.

However, several key challenges hinder the seamless adoption of IoMT in telemedicine:

1. **Interoperability Issues**: IoMT devices and telemedicine platforms, developed by various manufacturers, often face compatibility problems. This leads to fragmented data and communication failures, necessitating standardized protocols to ensure seamless integration.
2. **Heterogeneity of Devices and Protocols**: The wide variety of IoMT devices, each using different communication protocols and data formats, complicates their integration. Bridging these gaps is crucial for achieving seamless data exchange across systems.
3. **Scalability and Resource Management**: As IoMT adoption grows, managing large numbers of devices and vast amounts of data presents logistical and computational challenges. Effective scalability and resource management are essential for ensuring smooth operation in large-scale IoMT ecosystems.

This project aims to address these challenges by developing a scalable, interoperable solution that integrates IoMT with telemedicine, thereby improving healthcare delivery, enhancing patient services, and driving innovation in the medical field.

1.3 Justification of Study

The rapid expansion of telemedicine, accelerated by global health crises such as the COVID-19 pandemic, has exposed critical gaps in healthcare accessibility, particularly in underserved and remote regions. Addressing these gaps requires not only telemedicine platforms but also a seamless integration of various IoMT devices. This study is uniquely motivated by the urgent need to overcome interoperability challenges within these ecosystems, ensuring that patients can receive timely and high-quality care regardless of their geographical location.

By focusing on the development of an API-based interoperability solution, this research contributes a novel approach to unifying data from diverse IoMT devices, including wearables, sensors, and electronic health records (EHRs). Existing solutions often fail to achieve full compatibility across all platforms, limiting the potential of IoMT in improving patient outcomes. Our proposed solution builds on previous research but uniquely integrates open-source and commercial IoT platforms, leveraging middleware to ensure comprehensive device compatibility. This study's unique contribution lies in its practical and scalable approach to interoperability, providing a foundation that can be expanded upon in future telemedicine solutions. By solving this pressing issue, the research will contribute to a more integrated healthcare infrastructure and a more efficient, accessible healthcare system for all.

1.4 Aim and Objectives of the Study

The aim of this study is to develop a robust and scalable API-based interoperability solution for the Internet of Medical Things (IoMT) in telemedicine. This solution will enable seamless

communication, data exchange, and integration of diverse IoMT devices to improve healthcare delivery's efficiency and effectiveness.

To achieve the aim, the specific objectives are:

I. **Design a framework** for an API-based interoperability solution that ensures seamless data exchange and communication between diverse IoMT devices and telemedicine platforms.

II. **Develop and implement a prototype** of the proposed API-based interoperability solution, demonstrating its functionality and compatibility with various IoMT devices in a telemedicine use case.

III. **Evaluate the performance** of the developed solution by assessing device compatibility, communication efficiency, data accuracy, and system scalability in a simulated telemedicine environment.

1.5 Research Questions

How can an API-based interoperability solution be designed and implemented to integrate diverse IoMT devices with telemedicine platforms, ensuring real-time data exchange, device compatibility, and improved healthcare delivery?

1.5 Significance of the Study

The integration of the Internet of Medical Things (IoMT) into telemedicine, with a specific focus on healthcare affordability and improved services, holds immense significance in the contemporary healthcare landscape. This research study is significant for several reasons:

1. **Enhancing Healthcare Accessibility**: The study aims to make healthcare more accessible to a broader range of individuals, including those in underserved or remote

areas. By addressing affordability concerns, it can bridge healthcare disparities and extend services to those who previously had limited access to quality care.

2. **Improved Patient Outcomes**: Successful integration of IoMT in telemedicine has the potential to improve patient outcomes by enabling remote monitoring, timely interventions, and data-driven healthcare decisions. This can lead to better disease management and reduced healthcare costs in the long run.
3. **Cost Reduction**: By exploring cost-effective strategies for IoMT devices and telemedicine services, the study can contribute to lowering the financial burden on both healthcare systems and patients. Reduced costs can improve the sustainability of healthcare delivery models.
4. **Data Security and Privacy**: As the integration of IoMT involves the transmission and storage of sensitive patient data, addressing data security and privacy concerns is paramount. This study's findings can contribute to robust data protection mechanisms, fostering patient trust in IoMT-telemedicine systems.
5. **Technological Advancements**: The research can lead to technological advancements and innovations in computer science, particularly in the areas of data security, interoperability, and scalability. These advancements may have broader applications beyond healthcare.
6. **Policy and Industry Guidance**: The study's recommendations can inform policymakers, healthcare providers, and technology developers about best practices and regulatory guidelines for IoMT-telemedicine integration. This guidance can facilitate the responsible adoption of these technologies.
7. **Academic and Research Contribution**: The study contributes to the academic and research community by generating new knowledge and insights into the challenges and

solutions related to IoMT-telemedicine integration. It can serve as a foundational resource for future research in this field.

8. **Global Healthcare Impact**: The significance of this study extends beyond individual regions or countries. As IoMT and telemedicine are global phenomena, the findings can have a positive impact on healthcare systems worldwide, leading to more efficient and accessible healthcare services.
9. **Public Health Preparedness**: In times of health crises, such as pandemics, the integration of IoMT in telemedicine can play a crucial role in enhancing public health preparedness and response. This study can contribute to strengthening healthcare systems' resilience to emergencies.

The significance of this study lies in its potential to reshape the healthcare landscape by addressing affordability concerns, improving service quality, and leveraging technological innovations to benefit individuals, communities, and healthcare systems on a global scale.

1.6 Scope of the Study

The scope of this research study is defined by its primary focus on the integration of the Internet of Medical Things (IoMT) into telemedicine, with specific emphasis on healthcare affordability and the improvement of healthcare services. The study encompasses a range of components, including:

1. **Integration Framework**: The study delves into the development of a comprehensive integration framework for IoMT devices within telemedicine platforms. It explores the technical aspects of integrating diverse IoMT devices, sensors, and wearables into telehealth ecosystems.

2. **Data Security and Privacy**: The scope includes the design and implementation of robust data security and privacy measures to protect patient data within IoMT-telemedicine systems. It addresses encryption, authentication, access control, and compliance with privacy regulations.
3. **Interoperability Standards**: The study involves the establishment of interoperability standards and protocols to facilitate seamless communication and data exchange between IoMT devices and various telemedicine platforms. This encompasses the development of communication frameworks and compatibility solutions.
4. **Scalability Solutions**: Within the scope of this research, scalable infrastructure solutions are explored to efficiently manage the increasing volume of IoMT devices and data. It includes considerations for cloud computing, edge computing, and resource allocation strategies.
5. **Healthcare Affordability Strategies**: The study investigates strategies to enhance the affordability of IoMT devices and telemedicine services, with a focus on cost reduction without compromising quality care. This may involve the examination of open-source software, low-cost hardware, and telemedicine reimbursement models.
6. **Quality of Service Enhancement**: Within the study's scope, efforts are made to optimize the quality of telemedicine services. This includes addressing issues related to network performance, minimizing latency, and improving user interfaces for both patients and healthcare providers.
7. **Evaluation and Feasibility**: The research encompasses the assessment of the impact of proposed integration solutions on healthcare affordability, service quality, and

accessibility. It evaluates the feasibility of implementing these solutions in real-world healthcare settings.

8. **Policy and Recommendations**: The scope extends to providing recommendations based on research findings to inform policy decisions, industry practices, and healthcare delivery strategies in the context of IoMT-telemedicine integration.
9. **Academic Contribution**: The study contributes to the academic field by generating knowledge and insights into the challenges and solutions related to IoMT-telemedicine integration, potentially leading to further research and academic discourse.

It is important to note that while this study addresses a comprehensive range of issues related to IoMT-telemedicine integration, it may not cover all possible nuances or subdomains within these topics. The study's scope is defined by the primary objectives and research questions, with a focus on practical and impactful solutions within the domain of computer science and healthcare technology.

1.7 Limitations of the study

Hardware and Software Compatibility Problems

Due to variations in hardware specifications and software protocols, the interoperability solution encountered challenges when attempting to function across different IoMT devices. The study should outline the specific measures taken to address these issues and clarify how the remaining problems could affect the system's reliability. Unresolved issues may compromise the generalizability of the solution across various healthcare environments.

Data Privacy and Security Concerns

There are significant challenges in ensuring the privacy and security of sensitive medical data collected from IoMT devices, especially when transmitted through cloud applications. While efforts were made to comply with relevant regulations such as HIPAA, further discussion is needed regarding how these concerns were addressed. If these concerns were not fully resolved, they could affect the validity of the system in practical applications.

Reliability and Accuracy of Data Transmission

Despite implementing a robust system, issues such as network connectivity problems, device malfunctions, or other technical factors could still result in data transmission errors or inaccuracies. The study should provide further details on how these issues were mitigated and how remaining challenges could impact the overall accuracy of the system's performance.

Limited Scope of Testing Environments

The study's evaluation of system performance was constrained by the limited availability of real-world testing environments. The challenges faced in simulating diverse real-world scenarios should be discussed in more depth. These limitations may restrict the generalizability of the findings to broader contexts and affect the overall validity of the conclusions drawn.

User Acceptance and Usability

Usability and acceptance of the mobile application and cloud platform were found to vary among users, particularly healthcare professionals. The study should explore how these usability issues were addressed and identify any unresolved challenges. Failure to fully resolve these issues may affect the overall adoption and effectiveness of the interoperability solution in practice.

Resource Constraints

The study faced limitations in terms of time, budget, and human resources, which may have impacted the depth and breadth of the development, testing, and evaluation activities. Acknowledging how these constraints limited the study and what could not be fully explored due to them is essential for understanding the validity of the research findings.

1.8 Operational Definition of Terms

Affordability: Refers to the cost-effectiveness of healthcare services and technologies, ensuring they are accessible to individuals with limited financial resources.

Artificial Intelligence (AI): The simulation of human intelligence processes by software systems to perform tasks such as learning, reasoning, and problem-solving.

Data Analytics: The process of examining and analysing data to extract meaningful insights that support decision-making.

Data Exchange: Involves the transfer of healthcare information, such as patient records, test results, and diagnostic data, between different systems, devices, or entities within the healthcare ecosystem.

Data Security: Involves measures to protect data from unauthorized access, disclosure, alteration, or destruction, particularly relevant to safeguarding patient data in telemedicine systems.

Data Security and Privacy: Measures and protocols established to protect sensitive data from unauthorized access and to maintain the confidentiality of personal information.

Feasibility Analysis: Assesses the practicality and viability of implementing proposed solutions in real-world healthcare settings, considering technical, financial, and logistical factors.

Framework: A structured approach or set of guidelines used to address specific problems or challenges. In this study, it refers to a plan for integrating IoMT into telemedicine.

Healthcare Accessibility: Refers to the ease with which individuals can access healthcare services, factoring in geographical, financial, and physical considerations.

Health Recommender System: A software system that provides personalized healthcare recommendations to users based on the analysis of their data.

IEEE 802.16 Standards: A family of standards designed to provide long-range broadband wireless access (BWA) with quality of service (QoS) for different service levels, offering low latency, low jitter, low loss, and sufficient bandwidth.

Interoperability: The ability of software systems and devices to work together seamlessly and share data without compatibility issues.

Internet of Medical Things (IoMT): The application of Internet of Things (IoT) in the medical field, used for health monitoring and management through interconnected medical devices.

Internet of Things (IoT): A network of physical objects embedded with sensors and software, enabling them to connect and exchange data over the internet.

Policy Recommendations: Actionable suggestions based on research findings aimed at informing healthcare policies, regulations, and guidelines, particularly regarding IoMT-telemedicine integration.

Privacy: Refers to an individual's right to control the access and use of their personal information, particularly in the context of maintaining patient confidentiality in healthcare settings.

Quality of Service (QoS): Measures the performance and reliability of a service, particularly in terms of network connectivity, data transmission, and user experience. It is crucial for delivering high-quality telemedicine services.

Scalability: Refers to the ability of a system or infrastructure to handle increased workloads or user demands without compromising performance or stability. This is relevant to the expansion of IoMT-telemedicine ecosystems.

Telemedicine: The provision of remote healthcare services, including diagnosis, consultation, treatment, and monitoring, using telecommunications technology, allowing interaction between patients and healthcare providers without physical presence.

User Experience (UX): The overall experience a user has when interacting with a software or digital interface, particularly in terms of usability, functionality, and satisfaction.

Endnotes

1. S. B. Junaid, A. A. Imam, A. O. Balogun, L. C. De Silva, Y. A. Surakat, G. Kumar, M. Abdulkarim, A. N. Shuaibu, A. Garba, Y. Sahalu, A. Mohammed, T. Y. Mohammed, B. A. Abdulkadir, A. A. Abba, N. A. I. Kakumi & S. Mahamad. *Recent advancements in Emerging technologies for healthcare management systems: A survey.* **Healthcare**, 2022, 10(10), 1940. doi.org/10.3390/healthcare10101940

2. R. Dwivedi, D. Mehrotra & S. Chandra. *Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review.* **Journal of oral biology and craniofacial research**, 2022, 12(2):302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

3. S. Jain, M. Nehra, R. Kumar, N. Dilbaghi, T. Hu, S. Kumar, A. Kaushik & C. Z. Li. *Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases.* **Biosensors & bioelectronics**, 2021, 179, 113074. https://doi.org/10.1016/j.bios.2021.113074

4. V. K. Gunjan, V. G. Diaz, M. Cardona, M. Cardona, V. K. Solanki, K. V. N. Sunitha. *Remote Health Care System.* Applications to Electrical, Electronics and Computer Science and Engineering, 2020, 480-488. DOI: 10.1007/978-981-13-8461_54

5. W. E. Zhang, Q. Sheng, A. Mahmood, D. Tran, M. Zaib, S. Hamad, A. Aljubairy, A. Alhazmi, S. Sagar & C. Ma. *The 10 Research Topics in the Internet of Things*. 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, 34-43. doi:10.1109/CIC50333.2020.00015

6. J. Srivastava, S. Routray, S. Ahmad, & M.M. Waris. *Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress***.** Computational intelligence and neuroscience, 2022, 7218113. https://doi.org/10.1155/2022/7218113

7. S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, & L. Patrono. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. **Journal of cleaner production**, 2020, 274, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

8. F.M. Iqbal, K. Lam, M. Joshi, S. Khan, H. Ashrafian, & A. Darzi. *Clinical outcomes of digital sensor alerting systems in remote monitoring: A systematic review and meta-analysis.* **NPJ digital medicine**, 4(1), 2021, 7. https://doi.org/10.1038/s41746-020-00378-0

9. M. Osama, A.A. Ateya, M.S. Sayed, M. Hammad, P. Pławiak, A.A. Abd El-Latif, & R.A. Elsayed. Internet of Medical Things and Healthcare 4.0: *Trends, Requirements, Challenges, and Research Directions*. **Sensors (Basel, Switzerland)**, 2023, 23(17), 7435. https://doi.org/10.3390/s23177435-

10. J.N. S Rubí, & P.R. L Gondim. *IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR*. **Sensors (Basel, Switzerland)**, 2021,19(19), 4283. https://doi.org/10.3390/s19194283

11. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, & C. Douligeris. *Security in IoMT Communications: A Survey*. **Sensors (Basel, Switzerland)**, 2020, 20(17), 4828. https://doi.org/10.3390/s20174828

12. S. Tahir, S.T. Bakhsh, M. Abulkhair, & M.O. Alassafi. *An Energy-efficient Fog-to-Cloud Internet of Medical Things Architecture.* **International Journal of Distributed Sensor Networks**, 2022, 15(5), 1550147719851977.

13. R. Dwivedi, D. Mehrotra, & S. Chandra. *Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review*. **Journal of oral biology and craniofacial research**, 2022, 12(2), 302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

14. R. Dwivedi, D. Mehrotra, & S. Chandra. *Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review.* **Journal of oral biology and craniofacial research**, 2022, *12*(2), 302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

15. W. Glinkowski, K. Pawłowsk, & L. Kozłowska. *Telehealth and telenursing perception and knowledge among university students of nursing in poland*. **Telemedicine journal and e-health: the official journal of the American Telemedicine Association**, 2013, 19(7), 523–529. https://doi.org/10.1089/tmj.2012.0217

16. A.H. Mohd Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, & L.A. Latiff. *IoMT amid COVID-19 pandemic: Application, architecture, technology, and security*. **Journal of network and computer applications (Online)**, 2021, 174, 102886. https://doi.org/10.1016/j.jnca.2020.102886

17. K. Mohamed Akram, S. Sihem, K. Okba, & S. Harous. *IoMT-fog-cloud based architecture for Covid-19 detection*. **Biomedical signal processing and control**, 2022, 76, 103715. https://doi.org/10.1016/j.bspc.2022.103715

18. V. Kumar, M.S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, & A. Kumari. *RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure.* **The Journal of supercomputing**, 2022, 78(14), 16167–16196. https://doi.org/10.1007/s11227-022-04513-4

19. B.C. Uslu, E. Okay, & E. Dursun. *Analysis of factors affecting IoT-based smart hospital design.* **Journal of cloud computing (Heidelberg, Germany)**, 2020, 9(1), 67. https://doi.org/10.1186/s13677-020-00215-5

20. O. Pournik, T. Mukherjee, L. Ghalichi, & T.N. Arvanitis. *How Interoperability Challenges Are Addressed in Healthcare IoT Projects*. **Studies in health technology and informatics**, 2023, 309, 121–125. https://doi.org/10.3233/SHTI230754

21. T. Mazhar, A. Malik, S.A.H. Mohsan, Y. Li, I. Haq, S. Ghorashi, F. Karim, & S.M. Mostafa. *Quality of Service (QoS) Performance Analysis in a Traffic Engineering Model for Next-Generation Wireless Sensor Networks*. **Symmetry**, 2023, 15. doi:10.3390/sym15020513

22. P. Chanal, & M. Kakkasageri. Security and Privacy in IoT: A Survey. **Wireless Personal Communications**, 2020,115. doi:10.1007/s11277-020-07649-9

23. E.I. James, T.A. Murphree, C. Vorauer, J.R. Engen, & M. Guttman. *Advances in Hydrogen/Deuterium Exchange Mass Spectrometry and the Pursuit of Challenging Biological Systems.* **Chemical reviews**, 2022, 122(8), 7562–7623. https://doi.org/10.1021/acs.chemrev.1c00279

24. B. Nagajayanthi. *Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective*. **Wireless personal communications**, 2022, 123(4), 3661–3697. https://doi.org/10.1007/s11277-021-09308-z

25. P.K. Sadhu, V.P. Yanambaka, A. Abdelgawad, & K. Yelamarthi. *Prospect of Internet of Medical Things:* A Review on Security Requirements and Solutions. **Sensors (Basel, Switzerland)**, 2022, 22(15), 5517. https://doi.org/10.3390/s22155517

Chapter Two

Literature Review

2.1 Conceptual Review

2.1.1 Internet of Things (IoT)

With the incessant improvements in technology a prospective innovation, IoT is coming down the road which is growing as a universally worldwide computing system where everybody and everything will be linked to the Internet[1]. Imaginations are infinite which have put it on the edge of restructuring the present method of internet into an improved and incorporated form. The number of gadgets availing internet services is rising daily and having all of them linked by wire or wireless will put a powerful source of data at our fingertips. The idea of aiding communication between smart devices is an innovative technology but the technologies comprising the IoT are not something novel for us.

IoT, is the approach of combining information gotten from diverse types of items to any virtual platform on prevailing Internet setup[3]. The idea of IoT dates back to 1982 when an improved coke device was linked to the Internet which was able to tell the drinks contained and that whether the drinks were cold[4]. Later, in 1991, a modern-day vision of IoT in the form of global computing was first given by Mark Weiser[5]. Nevertheless in 1999, Bill Joy gave a clue about Device-to-Device interaction in his classification of internet[6]. In the same year, a researcher projected the word" Internet of Things" to designate a network of connected systems[7]. The basic concept of IoT is to allow automatic interaction of valuable data among imperceptibly entrenched different exclusively recognizable material world gadgets around us, powered by the principal technologies like Radio Frequency Identification (RFID) and Wireless Sensor

Networks (WSNs) which are sensed by the sensor systems and additional administered for decision making, on the foundation of which a computerized undertaking is executed.

The Internet of Things (IoT) is an emerging paradigm that enables many beneficial and prospective application areas, such as smart metering, smart homes, smart industries, and smart city architectures, to name but a few. These application areas typically comprise end nodes and gateways that are often interconnected by low power wide area network (LPWAN) technologies, which provide low power consumption rates to elongate the battery lifetimes of end nodes, low IoT device development/purchasing costs, long transmission range, and increased scalability, albeit at low data rates[2]

Additionally, Internet of Things (IoT) is a vibrant and worldwide system infrastructure, in which "Things"-subsystems and distinct physical and virtual objects—are recognizable, autonomous, and self-configurable.

"Things" are predictable to connect among themselves and network with the environment by exchanging information produced by detecting, while responding to happenings and generating actions to influence the material world.

The Internet of Things (IoT) is expanding into different aspects of our lives with technologies and applications in, for example, smart cities, healthcare, and smart homes. Tens of billions of objects are connected to the Internet, and the industry expects 50 billion IoT devices to existing by 2020. However, IoT devices are limited in resources such as storage and processing power, which impacts the performance, security, reliability, and privacy of IoT-based solutions and applications. Many applications are enhanced by integrating the IoT and cloud computing. Examples of such applications are in healthcare, smart cities, smart homes, smart metering [, video surveillance such as smart urban surveillance applications, agriculture, such as greenhouse

environment-monitoring system, and smart mobility, such as smart tourism destinations. Although IoT devices are limited in resources, cloud computing helps IoT in addressing such limitations[2].

IoT comprehends a sphere where billions of things can sense, interconnect and share data, all connected over public or private Internet Protocol (IP) systems. These connected things have information frequently collected, explored and used to initiate activities, providing a wealth of intellect for forecasting, administration and decision making. The IoT idea was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has lately become more applicable to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics"[10]. Internet of Things (IoT) ecosystem has a very composite project, in which numerous devices network with each other to facilitate innumerable solutions for the consumers. This is an inter-reliant scheme, which supports real-time information procurement, device connectivity, information transmissions, and analytics to influence consumers' demands. IoT delivers the linked surroundings, consist of the cyber physical systems, which incorporates human interpolation with computer-based devices and eases data-driven decision procedures[3].

Presently, IoT comprehends technologies such as smart homes, smart grids, intelligent logistics, and smart towns, augmented through sensor, actuator, and communication protocol networks. IoT delivers countless real-time responses through the integration of data analytics and sensors embedded on devices.

IoT has played an essential role in many industries over the last few decades. Recent advancements in the healthcare industry have made it possible to make healthcare accessible to more people and improve their overall health. The next step in healthcare is to integrate it with

IoT-assisted wearable sensor systems seamlessly[4]. This review rigorously discusses the various IoT architectures, different methods of data processing, transfer, and computing paradigms. It compiles various communication technologies and the devices commonly used in IoT-assisted wearable sensor systems and deals with its various applications in healthcare and their advantages to the world. A comparative analysis of all the wearable technology in healthcare is also discussed with tabulation of various research and technology. This review also analyses all the problems commonly faced in IoT-assisted wearable sensor systems and the specific issues that need to be tackled to optimize these systems in healthcare and describes the various future implementations that can be made to the architecture and the technology to improve the healthcare industry[5].

Again. IoT is a current communication model that predicts a near future in which the things of daily life will be fitted out with micro-controllers, transceivers for digital connection, and appropriate procedure stacks that will make them capable to connect with one another and with the consumers, becoming a vital fragment of the Internet"[18]. IoT is basically the moment in time when more "things or objects" were linked to the Internet than individuals[19]. The study summed that in 2003, there were about 6.3 billion individuals living on the globe and 500 million gadgets linked to the Internet which symbolized fewer than one (0.08) system for every individual. Based on Cisco IBSG's classification, IoT didn't hitherto exist in 2003 for the reason that the number of linked devices was comparatively minor given that universal gadgets like smartphones were just being introduced." "The IoT idea, therefore, intent in making the Internet even more immersive and prevalent. Moreover, by facilitating easy joining and communication with an extensive variation of gadgets like home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, etc., the IoT will support the improvement of number of devices that make use

of the potentially huge volume and variation of information produced by such items to deliver novel services to people, corporations, and public organizations. This paradigm certainly finds application in numerous diverse spheres, such as home computerization, medical aids, industrial automation, mobile health care, intelligent energy management and smart grids, elderly assistance, automotive, traffic administration and several others[20].

Figure 2.1: Internet of Things in Different Space[9]

Explosive evolution of smartphones and tablet PCs brought the number of gadgets linked to the Internet to 12.5 billion in 2010, while the global human populace rise to 6.8 billion, making the number of linked gadgets per individual more than 1 (1.84 to be exact) for the first time in history. The Internet doubles in magnitude every 5.32 years"[21]. It has been projected that by 2015 there will be 25 billion systems, 50 to 100 billion systems by 2020 linked to the Internet[22].

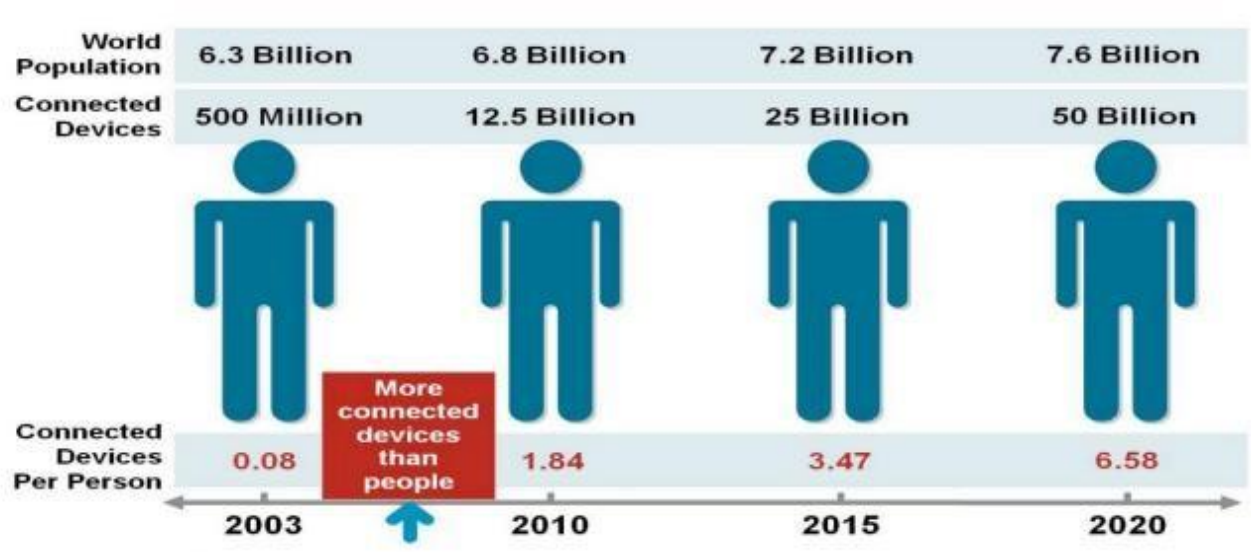


Figure 2.2: Expected Penetration of Connected Objects[8]

2.1.2 IoT Architecture

With the predicted development in IoT where more than 25 billion "things" are anticipated to be linked by 2020, Cisco states that this indicates enormous amounts that the current design of Internet with TCP/IP protocols will not handle. It was noted that with the swift growth of IoT there is need for novel open design that can address several security and Quality of Service (QoS) concerns along with support the prevailing system applications using open protocols. It was argued that without suitable assurance, IoT is not probable to be approved by many. Consequently, protection of information and privacy of users are main problems for IoT. More significantly, it was proposed that a number of multi-layered security designs for further advancement of IoT[9].

Authors termed a three vital level architecture of IoT whereas other authors defined a four vital level design[18]. Authors suggested a five layered design using the best features of the designs of Internet and Telecommunication management networks based on TCP/IP and TMN models

correspondingly. In the same way, authors summed a six-layered design based on the system classified structure[27]. So, in general it's classified into six layers as revealed in the Fig. 2.3."

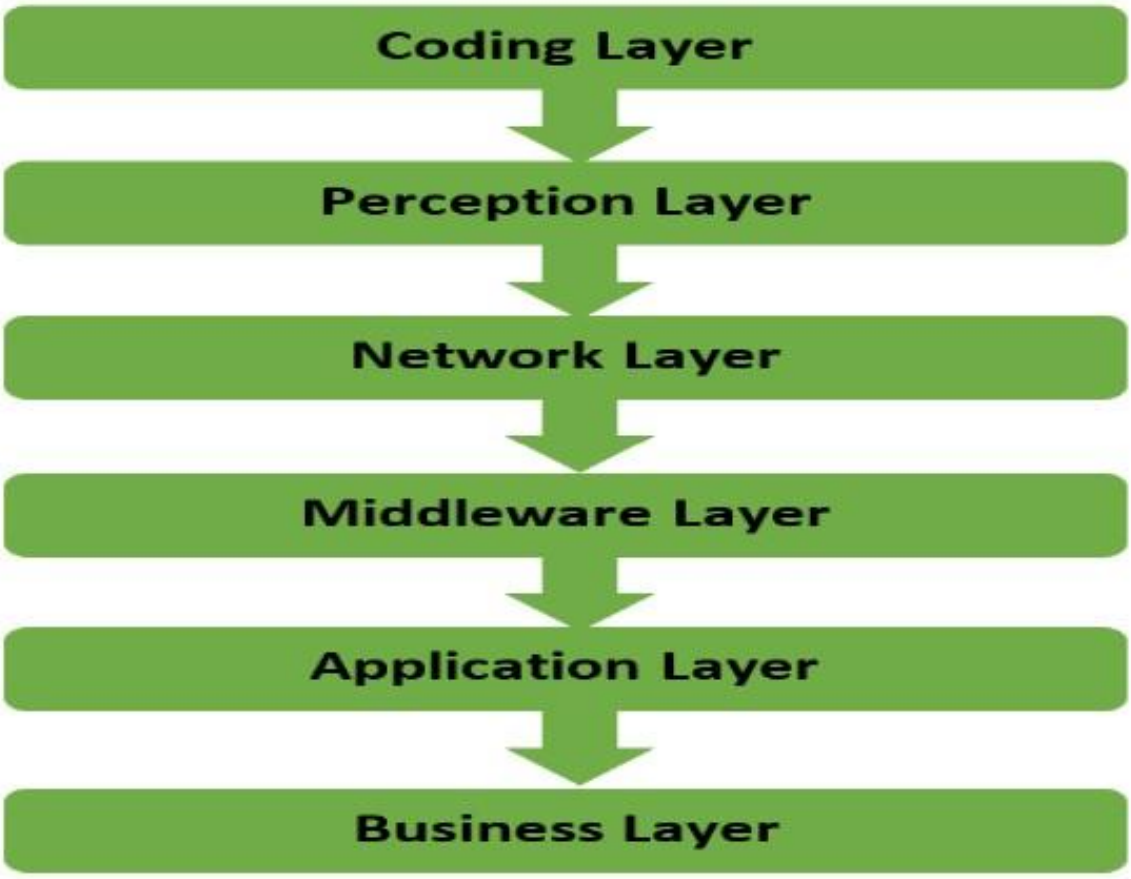


Figure 2.3: The six layers of IoT [9]

2.1.2.1 Coding Layer

Coding layer is the basis of IoT which delivers identification to the articles of interest. In this layer, each article is allocated a unique ID which makes it easy to recognize the objects[9]. Authors defines this layer as the foundation of IoT which provides identification to the objects of interest[10]. They summed that it is in this layer where every object is allocated an exceptional ID which makes it easy to differentiate the objects.

2.1.2.2 Perception Layer

This is the system interface of IoT which provides a bodily meaning to each object. It comprises of information sensors in diverse categories like RFID tags, IR sensors or other sensor systems[10] which could detect the humidity, temperature, speed, and place etc. of the items. This interface collects the valuable data of the items from the detected systems connected with them and changes the data into digital signals which is then passed onto the Network Layer for additional interaction. Authors summed that this is the device interface of IoT which delivers a bodily meaning to every item[30]. It comprises of information sensors in diverse forms like RFID tags, IR detectors or other detector systems which could detect the temperature, humidity, speed, and place etc. of the items. This interface collects the vital data of the items from the sensor devices connected with them and converts the data into digital signals which is then passed onto the Network Layer for further activities.

2.1.2.3 Network Layer

The aim of this layer is collecting the valuable data in the form of digital signs from the Perception Layer and communicate it to the dispensing devices in the Middleware Layer through the communication channels like Wi-Fi, Bluetooth, WiMAX, Zigbee, GSM, 3G etc. with procedures like IPv4, IPv6, MQTT, DDS etc[11].

2.1.2.4 Middleware Layer

This layer process the data obtained from the sensor devices[2]. It comprises the technologies like Cloud computing, Universal computing which ensures a direct access to the database to store all the essential data in it. Using some Smart Processing Equipment, the data is processed, and a completely computerized action is carried out based on the processed results of the data.

2.1.2.5 Application Layer

This layer recognizes the applications of IoT for all types of industry, based on the processed information. Because applications sponsor the advancement of IoT, so this layer is very helpful in the huge scale improvement of IoT system[9]. The IoT connected applications could be smart homes, smart transportation, smart planet etc.

2.1.2.6 Business Layer

This layer manages the applications and facilities of IoT and is answerable for all the study connected to IoT. It produces diverse business models for effective business schemes.

2.1.3 Technologies

The IOT was originally driven by members of the RFID community, who stated to the likelihood of ascertaining data about an identified object by browsing website or data bank entry that relates to a specific RFID or Near Field interaction technologies[33]. In the study, on research and application on the smart home based on element technologies and Internet of Things, the built-in main technologies of IoT are RFID, the sensor technology, nano technology and intelligence entrenched technology. Amongst them, RFID is the basis and interacting core of the architecture of Internet of Things[30].

RFID (Radio Frequency Identification) is a form of radio communication that involves the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. RFID technology use cases include healthcare, manufacturing, inventory management, shipping, retail sales, and home use. There are two common types of RFID. First, Active RFID tags contain the transmitter and power supply (battery) on board the tag. These are mostly UHF solutions, and reading ranges can extend up to 100 meters in some cases. Second, Passive RFID solutions, the reader and reader

antenna send a signal to the tag, and this signal is used to power the tag and reverse the power back to the reader. There are negative LF, HF and UHF systems[11].

The Internet of Things (IoT) allowed users to bring bodily items into the domain of cyber sphere. This was made conceivable by diverse classification devices like NFC, RFID and 2D barcode which permit material items to be recognized and referred above the web. IoT, which is incorporated with Sensor Technology and Radio Frequency Technology, is the universal system based on the ubiquitous hardware resources of Internet, is the Internet contents objects together. It is also a fresh upsurge of IT field since the usage of computing industries, communication system and universal roaming technology had been used. It comprises additionally to advanced technologies of computer and communication system outside, still comprising many novel backup technologies of Internet of Things, such as gathering Information Technology, Remote Communication Technology, Sea Measures Information Intelligence Analyzer, Remote Information Transmission Technology and Controlling Technology etc[12].

2.1.3.1 Radio Frequency Identification (RFID)

The most RFID systems consist of tags that are attached to the objects to be identified. Each tag has its own “read only” or “rewrite” internal memory depending on the type and application. A typical configuration of this memory is to store product information, such as an object's unique ID manufactured date, etc. The RFID reader generates magnetic fields that enable the RFID system to locate objects (via the tags) that are within its range. The high-frequency electromagnetic energy and query signal generated by the reader triggers the tags to reply to the query; the query frequency could be up to 50 times per second. As a result, communication between the main components of the system i.e. tags and reader are established. As a result, large quantities of data are generated. Supply chain industries control this problem by using filters that

are routed to the backend information systems. In other words, in order to control this problem, software such as Savant is used. This software acts as a buffer between the IT and the RFID reader [12].

2.1.3.2 Internet Protocol (IP)

Internet Protocol (IP) is the main system protocol used on the web, established in 1970s. IP is the principal interaction protocol in the Internet procedure suite for communicating datagrams across system boundaries. The two types of Internet Protocol (IP) are in use: IPv4 and IPv6. Every version defines an IP address otherwise. Because of its predominance, the generic term IP address stereotypically still denotes to the statements well-defined by IPv4. There are five categories of existing IP varieties in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are generally employed. The real protocol delivers for 4.3 billion IPv4 addresses whereas the IPv6 will meaningfully argue the availability to 85,000 trillion addresses[39]. IPv6 is the 21st century Internet Protocol. This supports around for 2128 addresses.

2.1.3.3 Electronic Product Code (EPC)

Electronic Product Code (EPC) is a 64 bit, or 98-bit code electronically recorded on an RFID device and projected to design a development in the EPC barcode scheme. EPC code can pile data about the kind of EPC, distinctive serial amount of product, its specifications, producer data etc. EPC was established by Auto-ID center in MIT in 1999. EPC global Organization which is accountable for standardization of Electronic Product Code (EPC) technology, produced EPC global Network[40] for sharing RFID data. It has four components namely Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS) and EPC Security Services (EPCSS)[35].

2.1.3.4 Barcode

Barcode is just a divergent way of encoding numbers and letters by using mixture of bars and spaces of varying width. Behind Bars[41] serves its original purpose to be expressive but is not precarious. In The Bar Code Book, it was recognized that there are other procedures of information entrance methods. Quick Response (QR) Codes the symbol for a kind of matrix barcode first intended for the locomotive industry in Japan. Bar codes are optical machine-readable labels attached to objects that gathered data connected to the article. Lately, the QR Code scheme has become widespread outside the locomotive industry owing to it sift readability and superior storage volume likened to standard. There are 3 kinds of barcodes of Alpha Numeric, Numeric and 2 Dimensional. Barcodes are considered to be device readable. Generally, they are read by laser scanners, they can also be read using a camera[36.]

A Barcode is a square or rectangular image containing a series of analogous black lines and white spaces of varying widths. Barcode is a machine-readable code in the form of numbers and an outline of parallel lines of varying widths, printed on a commodity. Hence a Barcode fundamentally is a way to encode information in a pictographic pattern that a machine can read. The combination of black and white bars signifies different text characters which follow a set algorithm for that particular Barcode[15].

2.1.3.5 Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) broadband network technology has made tremendous impact in the growth of broadband wireless networks. There exist today several Wi-Fi access points that allow employees, partners and customers to access corporate data from almost anywhere and anytime. Wireless broadband networks are expected to grow in terms of broadband speed and coverage, while Wi-Fi can be integrated with WiMAX networks to provide Internet connectivity to mobile

Wi-Fi users. This paper explores the Wi-Fi broadband wireless network technology, its uses, advantages and disadvantages, comparison with other broadband wireless networks and integration with WiMAX network[16].

Wireless Fidelity (Wi- Fi) is a networking technology that permits computers and other devices to communicate over a wireless sign. Vic Hayes has been termed as father of Wireless Fidelity. The precursor to Wi-Fi was in-vented in 1991 by NCR Corporation in Nieuwegien in the Netherland.

The first wireless devices were brought on the market under the term Wave LAN with speeds of 1 Mbps to 2 Mbps[37]. Today, there are closely pervasive Wi-Fi that provides the great speed Wireless Local Area Network (WLAN) connection to millions of offices, homes, and public locations such as hotels, cafes, and airports. The incorporation of Wi- Fi into notebooks, hand-helds and Customer Electronics (CE) machines has speeded the adoption of Wi-Fi to the point where it is closely a default in these machines[42]. Technology comprises any kind of WLAN product sustain any of the IEEE 802.11 alongside dual-band, 802.11a, 802.11b, 802.11g and 802.11n. At the moment, whole metropolises are becoming Wi-Fi corridors through wireless Aps[38].

2.1.3.6 Bluetooth

Bluetooth wireless technology is a low-priced, short-range radio technology that abolishes the need for proprietary cabling between gadgets such as notebook PCs, handheld PCs, PDAs, cameras, and printers and efficient range of 10 - 100 meters. Bluetooth gadgets are low-power and have a run of 10 meter remove from the gadget. Nowadays Bluetooth innovation is the usage of the convention characterized by the IEEE 802.15 standard. The standard characterizes a wireless PAN (Personal Area Network) operable in a zone of the measure of a room or a lobby.

It may be a convention of choice to associate two or more gadgets that are not in coordinate line of locate to each other. A security affiliation between two gadgets can be associated physically by matching the client entered common PIN (Personal Identification Number) number to each of the gadgets. When two gadgets endeavor to associate, unique key is created based on the PIN number entered on both the gadgets[17].

2.1.3.7 ZigBee

ZigBee is one of the procedures designed for improving the interface of wireless device systems. ZigBee technology is produced by the ZigBee Alliance which is established in the year 2001. Features of ZigBee are low cost, low data rate, comparatively short communication variety, scalability, dependability, elastic protocol interface. It is a low power wireless system procedure based on the IEEE 802.15.4 standard. ZigBee has variety of around 100 meters and a bandwidth of 250 kbps and the topologies that it works are star, cluster tree and mesh. It is broadly employed in home computerization, digital agriculture, industrial controls, medical monitoring & power systems. Numerous tiny, inexpensive, low-power devices known as sensor nodes make up a typical wireless sensor network. Typically immobile, these nodes interact with one another to acquire information about the surroundings. To track moving objects or enhance network coverage, these nodes might need to be made mobile in specific situations[39].

Wireless sensor networks (WSNs) are becoming increasingly important in human life and using in many fields such as agriculture, medical, military, etc. It includes densely allocated sensors for monitoring physical or environmental conditions, such as temperature, sound, pressure, and more. There are many communication technologies used in wireless sensor networks such as Wi-Fi, RF, Bluetooth, ZigBee. However, thanks to ZigBee's outstanding features such as energy-saving and long-distance transmission, it is always the first choice for applications in wireless sensor

networks. The WSNs includes a ZigBee coordinator (network coordinator), ZigBee Router, and ZigBee End-Devices. Information about the sensor nodes in the network is sent to the coordinator, the coordinator collects sensor data, stores the data in memory, processes the data, and routes the data to the appropriate node[40].

2.1.3.8 Near Filed Communication (NFC)

Near Field Communication (NFC) is a variety of short-range wireless technology at 13.56 MHz, naturally demanding a space of 4 cm. NFC technology makes life easier and more suitable for customers around the globe by making it simpler to make transactions, exchange digital content, and link electronic gadgets with a touch. Permits spontaneous initialization of wireless systems and NFC is corresponding to Bluetooth and 802.11 with their long-distance proficiencies at a distance circa up to 10 cm. It also works in filthy location, does not re-quire line of sight, easy and modest linking technique. It is first developed by Philips and Sony companies. Da-ta exchange rate nowadays approximately 424 kbps. Power consumption during data reading in NFC is under 15ma·

Similar to other identification technologies such as radio-frequency identification (RFID), barcodes, and QR codes, near-field communication (NFC) is a short-range (4–10 cm) wireless communication technology. NFC is based on the existing 13.56 MHZ RFID contactless card standards which have been established for several years and are used for payment, ticketing, electronic passport, and access control among many other applications. Data rates range from 106 to 424 kilobits per second. A few NFC devices are already capable of supporting up to 848 kilobits per second which is now being considered for inclusion in the NFC Forum specifications[20].

2.1.3.9 Wireless Sensor Networks (WSN)

A Wireless Sensor Networks (WSN) is a wireless system comprising of spatially dispersed autonomous devices using sensors to supportively track bodily or ecological circumstances, like temperature, sound, vibration, pressure, motion or pollutants, at different locations[45]. Fashioned by hundreds or thousands of motes that interact with each other and pass information along from one to another. A wireless sensor network is a significant component in IoT model. Sensor nodes may not have global ID for the reason that the huge amount of overhead and huge number of sensors.

Wireless sensor networks (WSNs) comprise a large number of sensor nodes which are generally used for various applications, such as target tracking, pressure monitoring, health monitoring, fire detection, and soon. The sensor nodes consist of transducers, radio transceiver, and wireless interfaces that are used together data from the environment. These inexpensive, small sensors form the network with group effort to perform the tasks as per their needs. To measure the change or property of environment, various kinds of sensor nodes such as biosensors and thermal, mechanical, magnetic, optical, and chemical sensors can be con-nested with node.1As sensor nodes consist of limited battery life, memory, processing power, and are installed at remote places (difficult to access), radio signal is used to perform the communication between the source and the base station[21].

2.1.4 Artificial Intelligence (AI)

Artificial Intelligence denotes to electronic atmospheres that are sensitive and reactive to the presence of individuals. In an ambient smart environment, systems work in concert to aid individuals in conveying out their daily life undertakings in easy, ordinary way using Data and

Intellect that is concealed in the system link devices. It is characterized by the following schemes of characteristics

(1) **Embedded:** Many Net- worked systems are incorporated in to the atmosphere.

(2) **Context Aware:** These systems can recognize you and your situational context.

(3) **Personalized:** They can be fashioned to your needs.

(4) **Adaptive:** They can change in reaction to you.

(5) **Anticipatory:** They can forestall your requests without conscious mediation.

2.1.5 Cloud Computing

Cloud is a paradigm shift in the Information and Communications Technology (ICT), through which businesses and users can have an on-demand network access to a shared pool of configurable computing resources (e.g. hardware, applications, services, etc.)[48,49]. Cloud computing model promotes broad network access to a pool of resources, optimal usage and control of resources, minimal management effort of hardware and software resources, scalable computing capabilities, and on-demand services without human interaction with service providers. Cloud computing provides new opportunities for CPSs in management and processing of aggregated sensor data and decision-making methods based on a cloud model allow CPSs to enhance the system capability.

During the last few decades, cloud computing has taken on several definitions. As per the National Institute of Standards and Technology (NIST), "Cloud computing is a service delivery model that facilitates easy, on-demand access to a shared pool of flexible computing resources that can be accessed and delivered on time with a minimum of effort or management" (NIST, as cited in Author, Year, p. X). As utility-based computing progresses, it is anticipated that it will move to cloud computing, which has the potential to be a more intelligent in-service provisioning

process. Another key advantage of cloud computing is that it reduces information technology (IT's) dependence on fundamental infrastructure settings (Author, Year, p. X). The implementation and execution of scientific workflows involving Big Data require a synergistic model, according to recent studies (Author, Year, p. X). Cloud computing has suggested the following functionality: measured services, rapid elasticity, scalability, multi-tenancy, resource pooling, extensive network access with on-demand service[22].

Cloud computing is a fundamental technology concept that plays a significant role in the integration of the Internet of Medical Things (IoMT) in telemedicine. Let's break down these two concepts and then explore their relationship:

Cloud computing refers to the delivery of computing services, including storage, processing power, and software applications, over the internet. Instead of relying on local servers or personal computers, cloud computing allows users to access and utilize these resources remotely, typically through a network of data centers managed by third-party providers. Cloud computing services are typically divided into three main service models:

a. **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet, including virtual machines, storage, and networking.

b. **Platform as a Service (PaaS):** Offers a platform for developing, deploying, and managing applications without worrying about the underlying infrastructure.

c. **Software as a Service (SaaS):** Delivers software applications over the internet, accessible through web browsers without the need for local installations.

2.1.6 Internet of Medical Things (IoMT):

IoMT is the extension of the Internet of Things (IoT) to the healthcare and medical field. It involves connecting medical devices, sensors, and equipment to the internet to collect, transmit, and analyses health-related data. IoMT devices can include wearables, remote monitoring devices, implantable sensors, and more. The primary goal of IoMT is to enhance healthcare by enabling real-time monitoring, data analysis, and remote patient care.

Now, let's explore the relationship between cloud computing and the integration of IoMT in telemedicine**:**

The integration of IoMT in telemedicine relies heavily on cloud computing for several reasons: **Data Storage and Processing**: IoMT devices generate a vast amount of healthcare data, such as patient vitals, diagnostic information, and treatment records. Cloud computing provides the scalable infrastructure and computing power needed to store, process, and analyse this data efficiently.

Accessibility: Cloud-based systems enable healthcare providers to access patient data and telemedicine platforms from anywhere with an internet connection. This remote accessibility facilitates telemedicine consultations, remote monitoring, and timely decision-making. **Security and Compliance**: Cloud providers often implement robust security measures and compliance standards to protect sensitive healthcare data. This is crucial for maintaining patient privacy and adhering to healthcare regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the United States.

Cost-Efficiency: Cloud computing allows healthcare organizations to pay for the resources they use, making it a cost-effective solution for managing IoMT data compared to building and maintaining on-premises infrastructure.

Scalability: As the demand for telemedicine and IoMT services grows, cloud resources can be easily scaled up or down to accommodate changing needs, ensuring seamless and reliable service delivery.

In summary, cloud computing serves as the backbone for the integration of IoMT in telemedicine by providing the necessary infrastructure, storage, processing capabilities, security, and scalability to effectively manage and utilize healthcare data for remote patient care and monitoring.

The integration of telehealth and cloud computing services promise to transform healthcare delivery to green areas while promoting and enhancing high-quality health outcomes.5,18–20 Figure 1 shows a pictorial representation of telemedicine services using cloud computing. The practice of telemedicine services helps to augment the shortage of skilled medical professionals, reduces referrals, increases quality of healthcare delivery, and bridges the barriers of access to healthcare for dwellers in underserved communities. Apart from the many promising benefits of telemedicine, there are still many hindrances and challenges to its adoption[24].

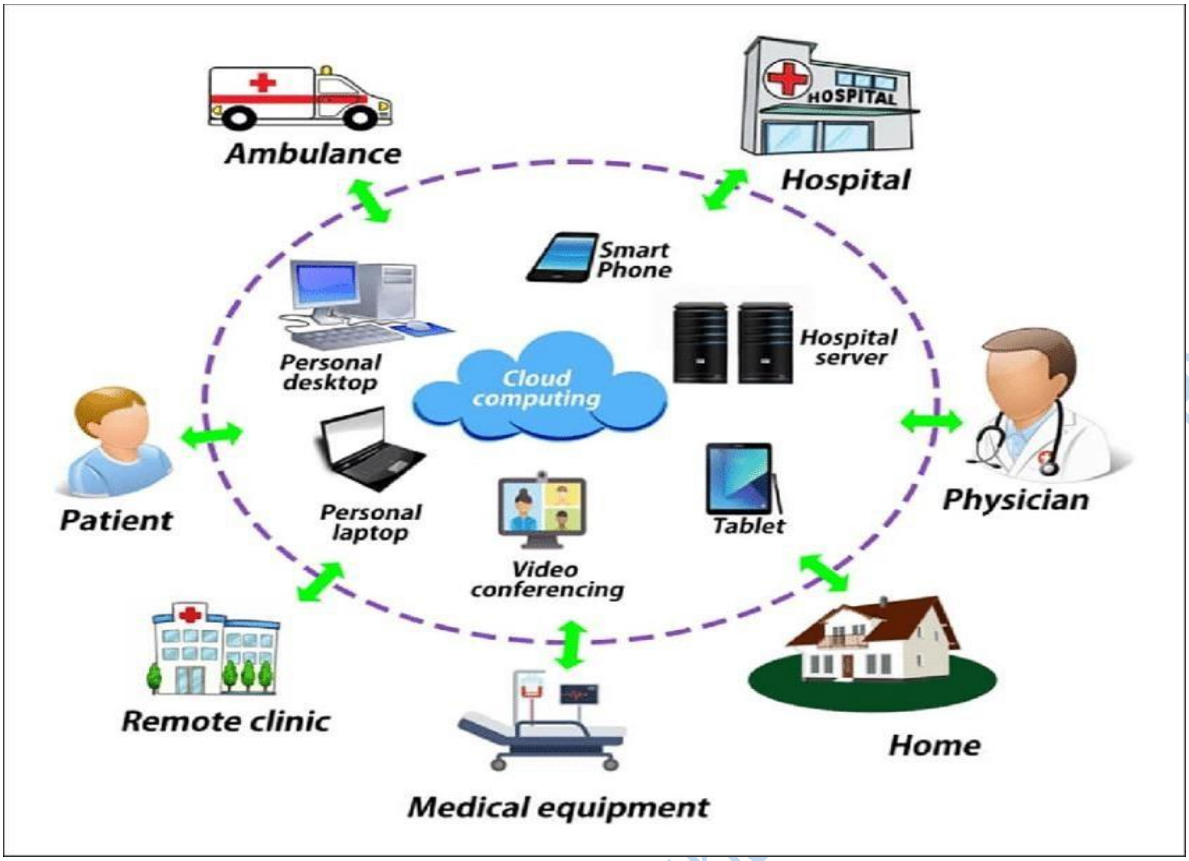


Figure 2.4: Telemedicine services based on cloud computing[24].

2.1.7 Components of Cloud Architecture:

The integration of the Internet of Medical Things (IoMT) in telemedicine relies on a cloud architecture that is specifically designed to support the storage, processing, and management of healthcare data. Here are the key components of cloud architecture in relation to IoMT integration in telemedicine:

(i) **IoMT Devices and Sensors**: These are the physical devices and sensors, such as wearable health trackers, medical monitoring devices, and IoT-enabled medical equipment, that collect health-related data from patients. These devices send data to the cloud for processing and analysis.

(ii) **Data Ingestion Layer:** This component handles the reception of data from IoMT devices. It includes mechanisms for data collection, data pre-processing, and data transformation to ensure that the data is in a usable format before storage and analysis.

(iii) **Data Storage:** This layer involves cloud-based data storage solutions, such as databases and data lakes, where healthcare data from IoMT devices is securely stored. Data may be structured (e.g., electronic health records) or unstructured (e.g., images, videos, or text notes).

(iv) **Data Processing and Analysis:** Cloud-based data processing tools and analytics platforms are essential for deriving meaningful insights from the collected healthcare data. Machine learning algorithms, artificial intelligence, and data analytics are often used to identify patterns, make diagnoses, and provide personalized recommendations.

(v) **Security and Compliance:** Ensuring the security and privacy of healthcare data is paramount. Cloud architecture should include robust security measures, encryption protocols, access controls, and compliance with healthcare regulations, such as HIPAA (in the United States) or GDPR (in Europe).

(vi) **APIs and Integration Layer:** APIs (Application Programming Interfaces) facilitate the integration of IoMT devices, telemedicine platforms, and healthcare systems with the cloud. This layer enables data exchange between different components and systems, ensuring interoperability.

(vii) **Telemedicine Platforms:** Telemedicine platforms are hosted in the cloud and enable remote patient consultations, video conferencing, and secure communication between healthcare providers and patients. These platforms often integrate with electronic health records (EHRs) and IoMT data for comprehensive patient care.

(viii) **User Interface (UI):** Cloud-based user interfaces, accessible through web browsers or mobile apps, allow healthcare providers and patients to interact with the telemedicine platform and access health information, appointments, and communication tools.

(ix) **Scalability and Elasticity:** Cloud architecture provides the flexibility to scale resources up or down based on demand. This ensures that the infrastructure can handle increased data flows and usage during peak times without performance degradation.

(x) **Monitoring and Management:** Cloud services often include monitoring and management tools to oversee the health and performance of the IoMT integration in telemedicine. This includes monitoring system uptime, resource utilization, and the ability to respond to issues proactively.

(xi) **Backup and Disaster Recovery:** Cloud-based solutions offer automated backup and disaster recovery capabilities to ensure data resilience and availability even in the event of hardware failures or natural disasters.

(xii) **Cost Management:** Cloud cost management tools and practices help organizations optimize their cloud expenses by monitoring resource usage, setting budgets, and identifying cost-saving opportunities.

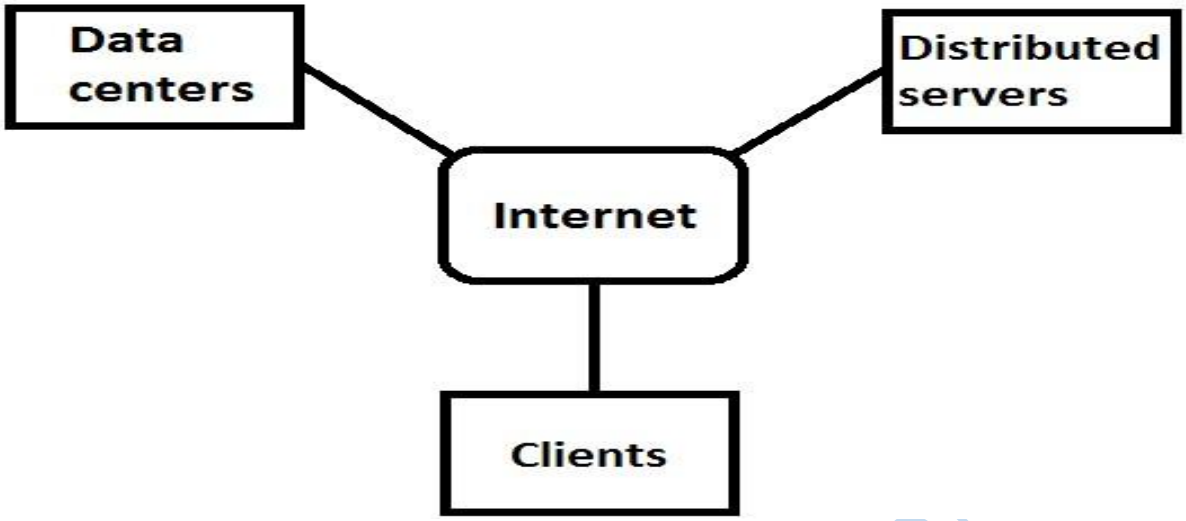


Figure 2.5:Simple Cloud Computing Network [25]

Cloud is not only simply collecting the computer resource, but also provides a management mechanism and can provide services for millions of users simultaneously. Nowadays, virtualization is entering every field of data center. It has become useful tool and improved service capacity. When the storage and computing capacity of the server cluster are surplus, we need not purchase servers, all we need to add a virtual machine running on the server [26].

2.1.8 Datacenters and Distributed Servers

In general, the data centers contain the services that clients want to obtain whenever they need it. This Centre is often a large space which contains all servers providing these services and keeping them up and running. It is also possible to have virtual servers which reduce the number of actual servers and space. Distributed servers are a name for those servers that are not all in one location.

It doesn't matter where these servers are, as a user you won't notice anything different. These kinds of servers provide high flexibility because it doesn't matter where they stand as long as they are connected to the internet. It is easy for making a back –up of other servers. Besides this, there is no limitation in expanding the cloud[58].

2.1.8.1 Clients

Most general clients are regular desktop PC's or laptops. Other clients nowadays are also mobile phones (PDA)[24]. The mobile devices are of big importance for cloud computing. They provide the high mobility to those who are trying to access the cloud. In general, there are three sorts of clients to distinguish. These are mobile, thin and thick clients. Mobile clients are those with mobile phones[58]. Thin clients are using remote hardware and software. What a user sees visualized by the server and not by an own hard disk with operating system. On the contrary, thick clients use own hard disks and usually access the cloud trough a web browser.

2.1.9.2 Users

Logically, behind the clients come the users. Without users, there is no purpose for a cloud. In cloud computing we can distinguish four different types of users. All these groups of users will be explained.

The groups to be distinguished as users in cloud computing are:

(i) Internet Infrastructure Developers

(ii) Service Authors

(iii) Integration and provisioning experts

(iv) End users

To point out the differences between the users and for the sake of understanding better what cloud computing is and how it is maintained, all users are explained. Even though for this thesis the focus lies on the end users it is important to distinguish these four kinds of users of the cloud.

i. **Developers**

The (Internet-infrastructure) developers in the cloud are those who develop and maintain the cloud. They have to guarantee and develop that all services get integrated[54]. Their

task is to provide end users with a simple interface, and keeping the complexity at a lower level.

ii. **Service Authors** These authors are somewhat different from the developers but in some cases have overlapping function. Where developers focus on providing all services, authors focus on individual services which may get used directly. Unlike the developers they don't need knowledge about technical specification of the cloud; they solely focus on providing easy to use services[61].

iii. **Integration and Provisioning Experts:** These experts are really more focused on the end-user solutions. They are trying to interface with end users, and try to meet in what end users want[24].

iv. **End Users:** The end users eventually have the highest importance as is mentioned before. End users expect that their cloud services have clear and easy to use interfaces, support and information provision. Also, the end users have to be protected from any hazard. Therefore, it is important to guarantee security in a cloud, something what will come up later in this thesis. All these requirements make no difference for the kind of users. Some users may hire cloud services for hours, and some for years. These different end-users should meet the same service as they could have equally important data streams into the cloud. The service also depends upon the Service Level Agreement. A Service Level Agreement (SLA) is included in a service contract between two parties. This agreement states what services are guaranteed by one party to the other. It states for example the performance agreements, but also more importantly the security and safety agreements.

2.1.9 Internet of Medical Things (IoMT)

The Internet of Medical Things (IoMT) refers to the connectivity of medical devices via the internet for data sharing purposes. It establishes links between medical devices, healthcare applications, and various health services to establish a smart healthcare infrastructure. All IoMT devices are linked to the cloud, where collected data are stored and analyzed. The IoMT has garnered significant attention from scientists and researchers, primarily due to the exponential growth in the number of interconnected medical devices and their capacity to generate, gather, and transmit data to the cloud for further analysis [28]. One of the key advantages of IoMT is its ability to facilitate accurate diagnoses, reduce treatment costs, and minimize errors. Health devices are paired with health applications, enabling individuals to share health data with healthcare providers for regular monitoring. Patients can communicate and remotely share their health data with healthcare professionals.

Internet of Medical Things (IoMT) shares several of the similar requirements as the conventional Internet of Things (IoT), particularly in terms of managing a huge number of gadgets, reliable communication, and system heterogeneity and interoperability. Internet of Medical Things (IoMT) is a healthcare scheme encompassed of intelligent medical gadgets and software applications. (IoMT) is proficient of giving remote medical analysis and opportune health services through the internet. IoMT, also recognized as healthcare IoT, refers to an increasing range of IoT applications in the medical sphere[60]. Sensors and software for remote healthcare tracking, telemedicine consultation, and delivery, for instance, are among the IoT devices and applications formed precisely for healthcare requirements and settings.

The growing connectivity of medical equipment has obvious implications for healthcare, including improved chronic-disease diagnosis and management for an aging global population.

According to a Deloitte report, more than 500,000 medical technologies are currently available. IoMT devices could be wearable and medical/vital monitors; strictly, they are intended to be used on bodies, in the household, community, clinic, or healthcare facilities for medical treatment; and they may include real-time location, telemedicine, and other services. The World Health Organization (WHO) defines e-health or IoMT as the application of information and communication technology (ICT) in the field of health. Electronic health records (EHR), patient health records (PHR), and mobile health are examples of subdomains within the e-health industry (m-Health). The Internet of Things (IoT) for health is widely used in e-Health areas. Figure 1 shows the security vulnerabilities of the IoMT environment. The environment consists of various healthcare instruments used to gather data; an Internet connection method; and the tool/software used to process, secure, send, and visualize information. Both wearable and implantable sensors collect data on the human body, send the data to a cloud server through the internet or using gateway, and the cloud server stores the data as a patient health information (PHI) file for further accessing by doctors/clinics[30].

The Internet of Medical Things (IoMT) refers to a network of interconnected devices linked to the internet, specifically designed to deliver healthcare services. Essentially, IoMT constitutes a connected ecosystem within the healthcare system, encompassing various medical devices, software applications, and services, as depicted in Figure 2.6. This interconnectedness allows for seamless communication between devices and sensors, empowering healthcare organizations to streamline their clinical operations and enhance workflow management. Moreover, it facilitates the remote monitoring of patient health, enabling healthcare providers to track patients' well-being from distant locations. IoMT serves as a bridge between the digital and physical realms, facilitating faster and more accurate diagnosis and treatment processes, ultimately leading to

improved patient health outcomes. Additionally, IoMT has the capacity to dynamically influence patient behavior and health status in real-time. The integration of medically relevant devices is poised to significantly impact both patients and clinicians alike[26].

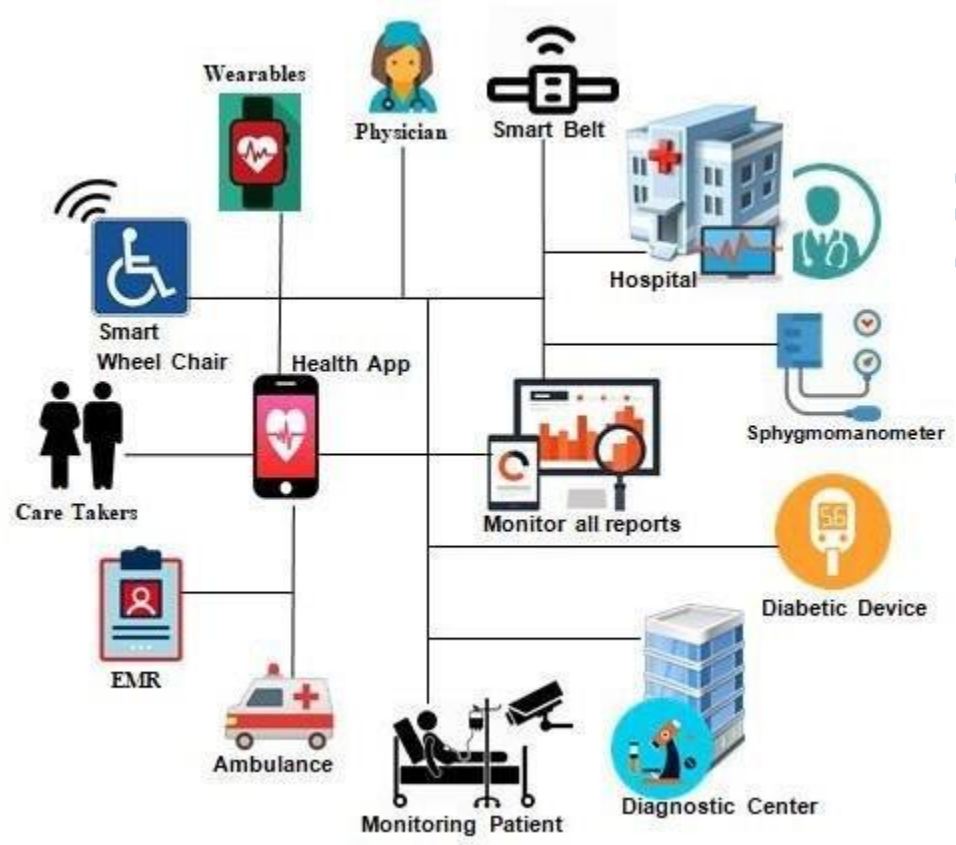


Figure 2.6: IoMT applications [26]

Internet of Medical Things (IoMT) is assisting individuals all over the global develop their health and access to medical services. IoMT also uses AI and machine learning to support life-changing changes to conventional medical apparatus, such as the smart inhaler for asthma sufferers[68]. In actuality, in the sense of body area networks, medical sensors and actuators are used as wearable gadgets. Rather than holding patients in hospitals, these systems can continuously track their health in real time while still providing them with better physical versatility and mobility. On the other, hand medical robots can be used as surgical robots as well as hospital robots[69], which are

capable of conducting small techniques with exactitude. They can also execute medical duties like cardiopulmonary resuscitation (CPR).

IoMT combinations conventional medical system reliability and protection with old-fashioned Internet of Things (IoT) dynamicity, genericity, and scalability capabilities[71]. It has the prospective to deal with the subject of ageing and chronic sicknesses by handling a huge amount of equipment for a huge number of patients. In addition, the IoMT deals with further problems like patient mobility.

Many services have been delivered by the IoMT technology, comprising improving healthcare services, data collection, disease management, patient experience, and low-cost services.

Furthermore, the Internet of Medical Things (IoMT) is a system of connected nodes in the healthcare segment, each of which is consist of a list of connected IoT devices, clinical systems, and wearable sensors. It improves the patient's care productivity as well as medical reaction times. Researchers presented a system based on cloud computing employing IoT sensors which is associated to the digital signature, time stamp mechanism and the asymmetric technology to monitor the other individual data[74]. This system is very effective in delivering medical services and utilizing less medical resources. Researchers explore the technical features of Internet of Things security briefly. Because when only two devices were combined in the sphere of medical care, security was a main problem. A general survey on medical large information analysis was executed in to sort large information problems and issues of adopting IoMT solutions[76]. Authors acknowledged generic concerns that add to a possibly insecure IoMT setting, like amalgamated reporting, context expertise, regulations, governance, resilience measures, standards, and technical controls. Researchers appraised technological developments made so far which can be utilized in IoMT and then investigated the concerns to be overcome. It was described that a

wireless sensor network health monitoring and alarm gadget that tracks, stores, and analyses body health data in order to send signals when suspicious behavior is detected. Authors presented a novel semantic model for patients' e-health based on current technologies, which are used to deploy IoT in the sphere of medical and intelligent health care. It comprises of an early wearable prototype for health monitoring that measures body temperature, heart rate, and fall detection to show these data on a Liquid Cristal Display (LCD) screen and send notifications to the nurse using a Global System for mobile communications (GSM) module.

Researchers introduced a dynamic L-RNN from artificial intelligence to recover missing information from IoMT applications to guarantee high quality of services to the end users[82].

Authors recommend the use of sensors entrenched in commercial mobile devices for uninterruptedly monitoring healthcare or ability on aged, owing to their attractive form influence and low power ingestion. Authors recognized several complications in the IoMT, where software implementation remains challenging[83]. By tracing vitals such as blood pressure, sugar levels, and uneven cellular development, Researchers suggested a healthcare monitoring system for rural people. Again, the Internet of Medical Things (IoMT) is a subset of the Internet of Things that is transforming the healthcare business. IoT sensor-based gadgets allow for incorporation with mobile technologies, which are referred to as Internet of Medical Things (IoMT)[85]. As the information gathered by these gadgets is pooled with electronic health record (EHR) systems, which capture vital information that is used to aid clinical resolution making, a fresh dimension is opened, and many potentials and uses arise through which this equipment can play a crucial part in changing contemporary healthcare systems, making them more functioning and tough.

Patients, visitors and medical personnel can all be trailed using IoMT-based technology, additionally improving the notion of smart hospitals. Actual patient tracking, innovative

diagnostics, robotic surgery, and other medical IoT applications will all help improve patient results. The situations that IoMT brings about comprise the proximity inferencing, location awareness, movement detection, and ecological sensing functionality. Medical findings information can now be collected and shared in unprecedented ways, saving time and money[86] and stimulating imminent promises.

IoMT is also vital in the progressively circulated nature of health and healthcare, as telemedicine and connected scientific improvements eradicate the need for office visits.

Internet of Medical Things (IoMT) is driving a healthcare development[87]. Patients and consumers yield from the use of connected web-enabled technologies. Through improved computerization, protection, and other scientific gains, IoMT offers novel prospects for healthcare workers to improve patient care and handle the intrinsic complication of the healthcare business.

2.1.10.1 IoMT Types

IoMT devices make available the needed or enhanced support for many medical disorders. The essential gadgets are implantable gadgets for specific medical disorders, e.g., pacemakers for heart illnesses. Conversely, the supporting equipment are typically wearables for enhanced healthcare experience, e.g., smartwatches. These disparities put the IoMT devices into two groupings, implantable medical devices (IMDs) and Internet of wearable devices (IoWDs).

Implantable Medical Devices (IMDs)

Any gadget that is entrenched to interchange, support, or improve a genetic design is an IMD. For instance, a pacemaker is an IMD that aids control irregular heartbeats, i.e., by sponsoring the heart to beat at a regular proportion if it is beating too fast or too slow[88]. Fig. 5 demonstrations various general IMDs and their situated positions in the human body. In recent times, wireless IMDs have been projected to unravel complications connected with wired IMDs, e.g., infection

and cable breakage[89]. IMDs are generally very minor and have very long battery lifespan. Therefore, low energy consumption, small storage space, and small batteries that last long are important requirements for these gadgets to stay inside a human body for a long time. For example, pacemaker implantations tend to last 5 to 15 years[31].

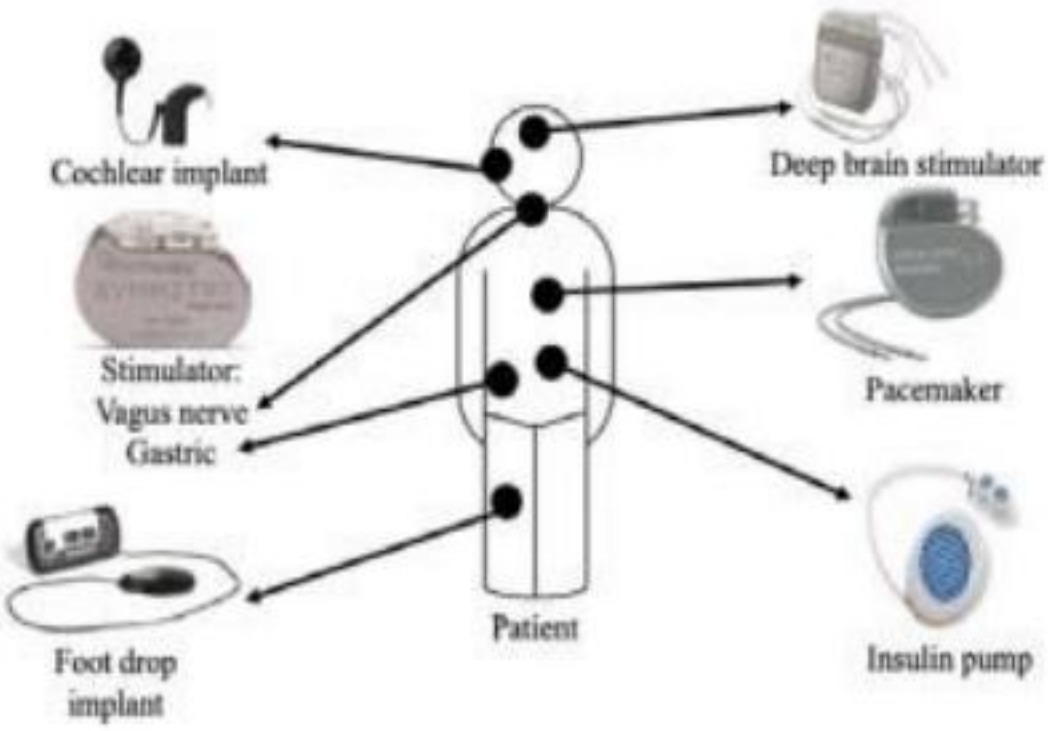


Figure 2.7: Examples of IMDs and their Locations in the Human Body [31]

Internet of Wearable Devices (IoWDs)

These are gadgets worn by people to observe their biometrics, e.g., heart rate, and may aid develop persons' general health. Instances comprise smartwatches, fall detection band, electrocardiogram (ECG) monitors, and blood pressure monitors[91]. Smartwatches are presently one of the most recognized forms of IoWDs to monitor biometrics such as heart frequency and flow. This observation can be employed to sense slow and fast heartbeats when the person is

inactive. The novel watches also aid fall recognition and ECG readings to notice atrial fibrillation (irregular heartbeat) health disorders. They are presently generally used for non-critical patient scrutiny. On the other hand, these gadgets have device precision and battery life constraints; consequently, not possible to replace IMDs in critical situations[93].

Figure 2.8: Showing Different wearable IoMT Devices [31]

2.1.9.2 IoMT Systems Architecture

Many of the contemporary IoMT devices are naturally separated into four layers, as shown in Fig 2.6. These layers comprise all information phases beginning from the person's biometric gathering stage and terminating in information storage and consequent visualization by a doctor for investigation. Furthermore, the patient can also imagine their general health status from the cloud. With the existing progresses in IMDs, IoWDs, and IMDs generally share the same design given that IMDs can connect with the portals, as demonstrated by Medtronic peacemaker[95].

2.1.10 Sensor Layer

This layer comprises of a set of petty entrenched or worn sensors that accumulate the patient's biometrics. The information is conveyed to the second layer over wireless protocols such as WiFi, Bluetooth, or over MEd Radio frequency spectrum reserved for IMDs.

(i) **Temperature Sensors:** These sensors monitor body temperature, room temperature, or the temperature of medical equipment. They are commonly used in fever monitoring, environmental monitoring in healthcare facilities, and incubators.

(ii) **Heart Rate Monitors:** Heart rate sensors can measure a patient's heart rate in realtime. They are often integrated into wearable devices, such as smartwatches and fitness trackers, to track physical activity and detect irregularities.

(iii) **Blood Pressure Sensors:** These sensors measure systolic and diastolic blood pressure. They are essential for managing hypertension and monitoring patients with cardiovascular conditions.

(iv) **Blood Glucose Sensors:** These sensors are used by individuals with diabetes to monitor their blood glucose levels. Continuous glucose monitoring (CGM) devices provide real-time data to manage insulin dosages.

(v) **Oxygen Saturation Sensors (Pulse Oximeters):** Pulse oximeters measure the oxygen saturation level in a patient's blood. They are used to monitor respiratory conditions and assess the need for supplemental oxygen.

(vi) Electrocardiogram (ECG or EKG) Sensors: **ECG sensors record the electrical** activity of the heart. They help diagnose arrhythmias, heart disease, and other cardiac conditions.

(vii) **Respiratory Rate Sensors:** These sensors monitor the number of breaths a patient takes per minute. They are used to assess respiratory conditions and detect abnormalities.

(viii) **Accelerometers**: Accelerometers are motion sensors that detect movement and acceleration. They are often integrated into wearable devices to track physical activity, falls, and patient mobility.

(ix) **Gyroscope Sensors:** Gyroscopes measure orientation and rotation. They are used in some wearable medical devices to monitor patient movements and balance.

(x) **Infrared Sensors:** Infrared sensors can measure body temperature and detect fever symptoms. They are commonly used in contactless thermometers and thermal imaging devices.

(xi) **Blood Flow Sensors:** These sensors measure blood flow in arteries and veins. They are used in vascular diagnostics and monitoring during surgical procedures.

(xii) **Scenography Sensors:** Capnography sensors measure the concentration of carbon dioxide (CO2) in exhaled breath. They are used in critical care settings to monitor respiratory function.

(xiii) **Ultrasound Sensors:** Ultrasound sensors are used for medical imaging to visualize internal organs, tissues, and fetuses during pregnancy.

(xiv) **Electromyography (EMG) Sensors:** EMG sensors record the electrical activity of muscles and nerves. They are used in neuromuscular diagnostics and rehabilitation.

(xv) **Environmental Sensors:** These sensors monitor factors like air quality, humidity, and radiation levels in healthcare facilities to ensure patient safety and comfort.

(xvi) **Pressure Sensors**: Pressure sensors measure force or pressure changes and are used in devices like ventilators, infusion pumps, and arterial catheters.

(xvii) **Light Sensors**: Light sensors can measure light intensity and UV radiation exposure. They are used in phototherapy devices and UV radiation monitoring.

These sensors, when integrated into IoMT devices and systems, provide healthcare professionals with real-time data for diagnosis, treatment, and remote patient monitoring. The continuous advancement of sensor technology is expanding the possibilities for improving patient care and medical research in the IoMT ecosystem.

2.1.11 Data Format

Choosing the right data format is essential for interoperability between different healthcare systems and devices on the Internet of Medical Things (IoMT), various data formats are used to represent and transmit medical information collected from devices and sensors. These data formats ensure interoperability, data integrity, and security in IoMT applications. Here are different types of data formats commonly used in IoMT devices

HL7 (Health Level Seven)

HL7 is a widely adopted standard for exchanging electronic health information. It defines structured messages and documents for clinical and administrative data. Versions such as HL7 v2.x and HL7 FHIR (Fast Healthcare Interoperability Resources) are commonly used in healthcare.

DICOM (Digital Imaging and Communications in Medicine)

DICOM is a standard for storing, transmitting, and sharing medical images and associated information. It is essential for medical imaging devices like X-ray machines, MRI scanners, and PACS (Picture Archiving and Communication Systems).

XML (Extensible Markup Language)

XML is a versatile markup language used for structuring and encoding healthcare data. It allows data to be easily parsed and exchanged between systems. Many healthcare standards, including HL7 and CDA (Clinical Document Architecture), use XML.

JSON (JavaScript Object Notation)

JSON is a lightweight data-interchange format commonly used in IoMT applications. It is human-readable, making it suitable for data exchange between web-based systems and mobile apps.

EDIFACT (Electronic Data Interchange for Administration, Commerce, and Transport)

EDIFACT is a standard for electronic data interchange (EDI) in various industries, including healthcare. It defines message formats for exchanging administrative and financial data.

CSV (Comma-Separated Values)

CSV is a simple text-based format for tabular data. It is often used for exporting and importing healthcare data, such as patient lists and laboratory results.

JSON-LD (JSON for Linked Data)

JSON-LD is a JSON-based format for representing linked data on the web. It is used to structure healthcare data in a way that is both human-readable and machine-understandable.

Raw Data Formats

Some medical devices and sensors produce raw data formats specific to their manufacturers. These formats may require custom parsers to extract meaningful information.

Custom Binary Formats

Some proprietary IoMT devices use custom binary formats for efficiency and data security. Reverse engineering may be required to interpret data from such formats.

XML-Based Standards

IoMT may use XML-based standards like CDA (Clinical Document Architecture) and CCD (Continuity of Care Document) for patient records and summaries.

EHR (Electronic Health Record) Formats):

Various EHR vendors use their own data formats for storing patient records. These formats may conform to industry standards or be proprietary. Choosing the appropriate data format depends on factors like the type of medical data, system compatibility, and interoperability requirements. Standards such as HL7, DICOM, and FHIR play a vital role in ensuring consistent and secure data exchange in the IoMT ecosystem.

2.1.12 IoMT Data Security

IoMT data security is critical to protect patient privacy and ensure the integrity and confidentiality of medical data. It involves encryption, access control, authentication, and secure data transmission practices. Compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) is vital. Security is a critical aspect of the Internet of Medical Things (IoMT) to ensure the confidentiality, integrity, and availability of healthcare data and devices. There are several types of data security measures and technologies used in IoMT devices:

1. **Encryption:** Data Encryption: Encryption techniques such as SSL/TLS are used to secure data transmission between IoMT devices and servers, protecting data from eavesdropping.
2. **Storage Encryption:** Data stored on IoMT devices or in cloud storage is often encrypted to prevent unauthorized access in case of device theft or data breaches.
3. **Access Control:** User Authentication: Secure login mechanisms, including usernames, passwords, and multi-factor authentication (MFA), restrict access to authorized personnel.

4. **Role-Based Access Control (RBAC):** Role-based access ensures that users can only access data and perform actions based on their roles and permissions.
5. **Data Integrity:** Digital Signatures: Digital signatures verify the authenticity and integrity of transmitted data, ensuring that it has not been tampered with during transit.
6. **Checksums and Hashing:** Checksums and cryptographic hashing are used to detect changes or corruption in data.
7. **Firewalls and Intrusion Detection Systems (IDS):** Firewalls and IDS protect IoMT networks from unauthorized access and monitor for suspicious activities or intrusion attempts.
8. **Device Authentication and Authorization:** Devices should be authenticated before connecting to a network or other devices to prevent unauthorized devices from joining the network. Authorization mechanisms ensure that devices can access only the resources they are allowed to.

2.1.12.1 Secure Boot and Firmware Updates

Secure boot processes verify the integrity of device firmware during startup, ensuring that it has not been compromised.

Regular firmware updates are essential to patch security vulnerabilities and protect against known threats.

2.1.12.2 Physical Security

Physical safeguards, such as locks, biometric access controls, and tamper-evident packaging, protect IoMT devices from physical attacks and unauthorized access.

2.1.12.3 Secure APIs

Application Programming Interfaces (APIs) used for data exchange between IoMT devices and systems should be secured to prevent unauthorized access or data leakage.

1. **Data Masking and Redaction:** Sensitive data can be masked or redacted to protect patient privacy and comply with regulations like HIPAA (Health Insurance Portability and Accountability Act).
2. **Security Information and Event Management (SIEM):** SIEM tools collect and analyze security data from IoMT devices and networks to identify security incidents and threats.
3. **Remote Wipe and Kill Switch:** In case of device loss or theft, the ability to remotely wipe data or disable a device (kill switch) can prevent unauthorized access to sensitive information.
4. **Secure Communication Protocols:** The use of secure communication protocols, such as HTTPS, MQTT-TLS, and CoAP-DTLS, ensures that data is transmitted securely between devices and servers.

(i) **Network Segmentation:** Network segmentation isolates IoMT devices from other parts of the network, reducing the attack surface and limiting lateral movement of threats.

(ii) **Security Auditing and Compliance:** Regular security audits and compliance assessments help ensure that IoMT systems adhere to security best practices and regulatory requirements.

(iii) **Data Backup and Recovery:** Regular data backups and disaster recovery plans protect against data loss due to security incidents or system failures.

(iv) **Behavior Analytics:** Behavioral analysis tools monitor device and user behavior to detect anomalies and potential security breaches.

(v) **End-of-Life (EOL) Planning:** Planning for the secure disposal or decommissioning of IoMT devices at the end of their lifecycle prevents data exposure.

(vi) **Vulnerability Management:** Continuous monitoring and patching of vulnerabilities

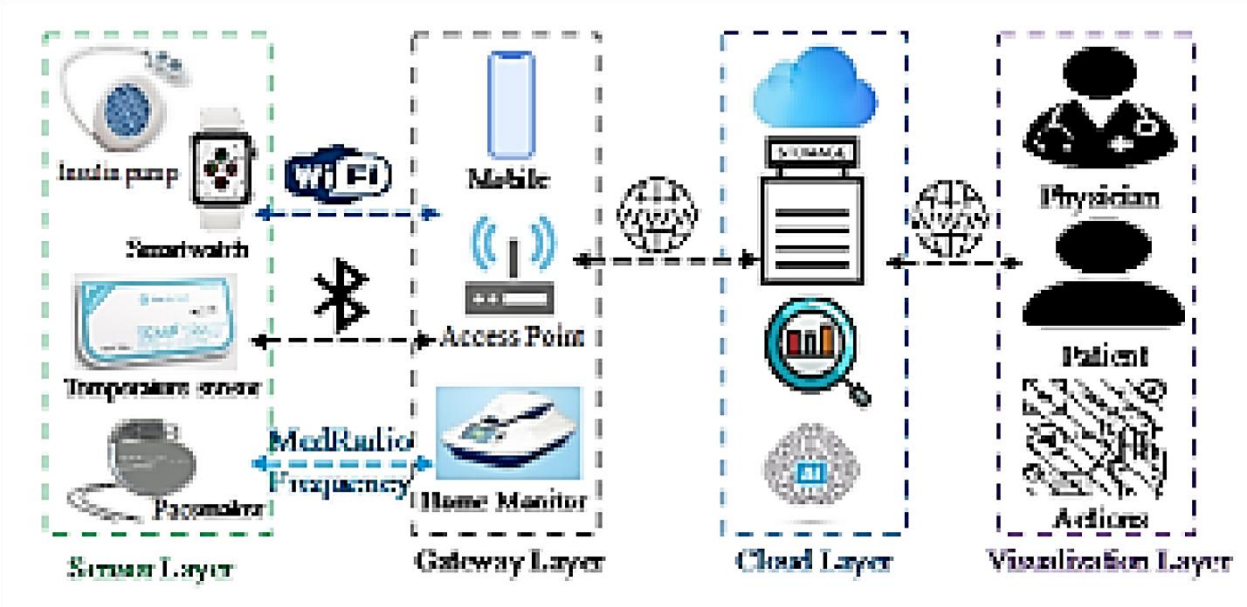


Figure 2.9: Fig IoMT devices and software are essential to address emerging threats [14]

(vii) **Regulatory Compliance:** Compliance with healthcare data security regulations such

2.1.13 Gateway Layer

Due to the handling and storage limitations of IoMT devices, the information is transmitted without processing to the second layer, i.e., the gateway layer. The gadgets in this layer can be the patient's smartphone or an assigned access point (AP), which are commonly more potent than sensors. They can execute some preprocessing processes, like authentication, short term information storage, and simple AI-based analysis. Additionally, they transmit the sensor information to the cloud over the Internet.

IoMT Gateway Layers

(i) **IoMT Device Communication**: The gateway will be responsible for establishing secure and efficient communication channels with IoMT devices, which could include various types of medical sensors and equipment.

(ii) **Data Aggregation**: The gateway should aggregate data from multiple IoMT devices. This could involve collecting data from different types of sensors and ensuring that it is transmitted in a consistent format.

(iii)**Local Processing:** Depending on the project's requirements, the gateway may perform local data processing tasks. For example, it might filter or preprocess data before forwarding it to backend systems or Communication System.

(iv) **Security**: Ensuring data security is paramount. The gateway should implement robust security measures to protect sensitive medical data during transmission and storage. This includes encryption, authentication, and access control.

(v) **Interoperability**: While the gateway is limited to IoMT, it should still consider interoperability. Ensure that it can communicate with different types of IoMT devices and potentially conform to standardized healthcare data formats like HL7 or FHIR for compatibility with other healthcare systems.

(vi) **Scalability**: Design the gateway to be scalable, allowing it to handle a growing number of IoMT devices efficiently.

(vii) **Integration**: If necessary, the gateway might need to integrate with specific IoMT backend systems, such as Electronic Health Records (EHRs) or cloud-based healthcare platforms.

(viii) **Compliance**: Ensure that the gateway adheres to relevant regulations and standards for medical devices and data, such as HIPAA or GDPR, depending on your project's geographical scope.

(ix) By focusing the IoMT gateway on IoMT-specific functions, you can create a specialized and tailored solution that effectively manages IoMT device communication, data handling, and security within the healthcare context. This approach allows for a more efficient and secure healthcare IoT ecosystem.

2.1.14 Cloud Layer

Designing a cloud layer for collecting medical data from various IoMT (Internet of Medical Things) devices involves creating a scalable and secure cloud-based infrastructure that can receive, process, store, and manage data from these devices. Below is an outline of the components and considerations for such a cloud layer:

(i) **Cloud Infrastructure:** Choose a cloud service provider (e.g., AWS, Azure, Google Cloud) to host your cloud-based solution. Set up the necessary virtual machines, containers, or serverless functions to handle incoming data.

(ii) **API Gateway**: Implement an API gateway (e.g., AWS API Gateway, Azure API Management) to manage incoming requests from IoMT devices. The API gateway can route requests to the appropriate services and enforce security policies.

(iii) **Authentication and Authorization:** Implement robust authentication and authorization mechanisms. Ensure that only authorized devices and users can access the API. OAuth 2.0 and JWT (JSON Web Tokens) are common choices for securing APIs.

(iv) **Data Ingestion:** Create data ingestion pipelines to receive data from IoMT devices. This can be done through RESTful APIs, MQTT for IoT devices, or other suitable protocols.

Ensure that data transmission is secure (e.g., HTTPS) and can handle large volumes of data.

(v) **Data Transformation**: Depending on the format of data generated by IoMT devices, you may need to transform it into a standardized format (e.g., HL7, FHIR) for consistency and compatibility with healthcare systems.

(vi) **Data Processing**: Implement data processing logic to clean, validate, and enrich incoming data. You might need to perform real-time analytics, anomaly detection, or aggregation based on your project requirements.

(vii) **Storage**: Choose appropriate storage solutions (e.g., databases, data lakes) to store IoMT data securely. Consider both structured and unstructured data storage needs. Ensure compliance with data retention and privacy regulations.

(viii) **Scalability**: Design the cloud layer for horizontal scalability to accommodate an increasing number of IoMT devices and growing data volumes. Use auto-scaling and load balancing to handle spikes in traffic.

(ix) **Monitoring and Logging:** Implement monitoring and logging solutions (e.g., AWS CloudWatch, Azure Monitor) to track system performance, detect anomalies, and troubleshoot issues in real-time.

(x) **Security**: Implement robust security practices, including encryption of data at rest and in transit, regular security audits, and access control mechanisms to protect sensitive medical data.

(xi) **Compliance**: Ensure compliance with healthcare data regulations, such as HIPAA (for the United States) or GDPR (for the European Union), depending on your project's geographical scope.

(xii) API Documentation: Create comprehensive API documentation for developers and device manufacturers, detailing how to connect their devices to your cloud-based API.

(xiii) **Integration**: Plan for integration with other healthcare systems, such as Electronic Health Records (EHRs) or telemedicine platforms, to provide a holistic view of patient data.

(xiv) **Data Analytics**: Implement data analytics and reporting capabilities to derive insights from the collected medical data, which can be valuable for healthcare providers and researchers.

(xv) By carefully designing and implementing each of these components, your cloud layer can serve as a robust and scalable foundation for collecting medical data from various IoMT devices, contributing to improved patient care and healthcare research.

2.1.15 Visualization/Action Layer

In this layer, the information is accessible to the doctors and the patients to track their healthiness. This layer also comprises the activities suggested by the doctor based on the patient's fitness situations. Instances of activities comprise recommending or regulating the prescription for numerous drugs.

2.2 IOMT Security Model

In this segment, we deliberate the dangers to the IoMT devices' information at three diverse phases. Similarly, we present the IoMT devices' safety requirements and commonly classify countermeasure procedures. In succeeding segments, every countermeasure classification will be additionally detailed with its connected procedures and employ in IoMT devices.

2.2.1 IoMT Dangers at Diverse Stages

IoMT devices must shield the patients' information at all phases, comprising collection, communication, and storage. these phases comprise of incorporations of the four design layers.

1) Data Collection

The gathering of the patient's information in the sensor layer is the first phase of an IoMT device. Attacks at this phase can be software (i.e., data tampering) or hardware (i.e., sensor hardware manipulation) attacks. These attacks can threaten patients' wellbeing if the sensor hardware or software is affected. Therefore, shielding the information against these assaults is important to keep the system running.

2) Data in Transit

This phase comprises interactions between the gadgets in all four layers, e.g., the interactions between the IoMT sensors in the sensor layer and the AP in the portal layers. Attacks here can influence or block the sensor data being communicated. Thus, safeguarding against these assaults would avert the information from being manipulated while being transmitted among the four layers.

3) Data in Storage

Once the patient's information is composed and communicated from the sensor and portal layers, they are kept in the cloud layer. Assaults in this layer differ from theft account authorizations to DoS/DDoS assaults. Shielding the information in this layer and the picturing layer from any illegal entree is vital. This is serious since, in this layer, most of the information are inactive most of the time; hence, they are at more danger than any other phase.

2.2.2 IoMT Security Requirements

Owing to the patient information sensitivity and security, a set of requirements that can safeguard IoMT devices' safety at all layers is required. The set has been derived from CIANA considerations and comprises of the following safety requirements[97, 98]

1) Confidentiality/Privacy

The capacity to keep the information secretive while being collected, communicated, or kept. Additionally, they must only be available to accredited users. The most common procedures to achieve this condition are information encryption and entree control lists, which will be deliberated further in the subsequent segment.

2) Integrity

This is connected to the capacity to shield the information from any illegal interfering during the gathering, transmission, and storage phases.

3) Availability

The capability to properly retain the IoMT devices uninterruptedly running. This can be achieved by keeping the device up to date, monitoring any variations in their execution, providing redundant information storage or communication pathways in instance of DoS assaults, and correcting any error as soon as possible.

4) Non-Repudiation

The capability to make every official user accountable for his/her actions. In other words, this condition assures that any communication in the device cannot be denied. This can be accomplished using digital signature procedures.

5) Authentication

The capacity to authenticate the individuality of a handler logging on the device. Mutual verification is the safest method where both the server and the customer validate each other before securing data/key conversation.

6) Authorization

The capacity to permit authentic handlers to only implement directives to which they are certified. Comparable to confidentiality, authorization can be accomplished using appropriate information encryption and entree control procedures.

7) Anonymity

The capacity to retain the patients'/physicians' personalities concealed from illegal handlers when they interrelate with the device. Using smart cards can achieve the privacy condition.

8) Forward/Backward Secrecy

This makes available the capacity to retain imminent communicated information/secrets safe even if old information/ keys compromised. Backward secrecy makes sure the reverse, where old information/keys are safe even if an attack has fruitfully affected existing information/secrets. Forward/Backward secrecy can be realized by time-based verification factors, e.g., time-based keys that can be created and used only when clock time at both nodes tie.

9) Secure Key Exchange

The capacity to firmly share the keys among the nodes in the device. Diffie-Hellman key exchange is a sample of a protected key exchange.

10) Key-Escrow Resilience

The system admin cannot imitate any certified handler in the device. This guards against inside dangers. Utilizing asymmetric keys with a cryptographic hash function (CHF) can achieve this condition.

11) Session Key Agreement

The nodes in the device must employ session keys after the verification procedure. Comparable to key-escrow flexibility, engaging symmetric/asymmetric keys with CHF can achieve this condition. The main motivation of the research work is that WSN monitors different activities; most of them are very sensitive. Therefore, we need a robust security scheme for these activities. In the paper, a cryptographic technique to protect sensitive applications for different applications. However, robust security algorithms need much recourse, such as adequate memory, bandwidth, and energy resources. Therefore, it is challenging to apply any robust cryptographic algorithm in a resource constraint WSN that reduces their sources' capabilities. Furthermore, trust management between sensor nodes with crucial management in a dynamic environment performs packet delivery and average delay. Moreover, the privacy of data is efficiently protected[42].

2.2.2 IoMT Systems Security Techniques

There are numerous diverse procedures to protect IoMT devices. These methods can be separated into three major classifications: symmetric, asymmetric, and keyless, as shown in Fig 2.10. Symmetric and asymmetric procedures depend on cryptographic algorithms, while keyless procedures are noncryptographic. The cryptographic procedures comprise one-factor and two factor verification procedures, which are explained in the next three segments.

One-factor verification engages only one verification procedure to guard the system. In contrast, two-factor authentication adds a second verification procedure (factor), such as biometrics, to guard the device if one of the two elements is compromised.

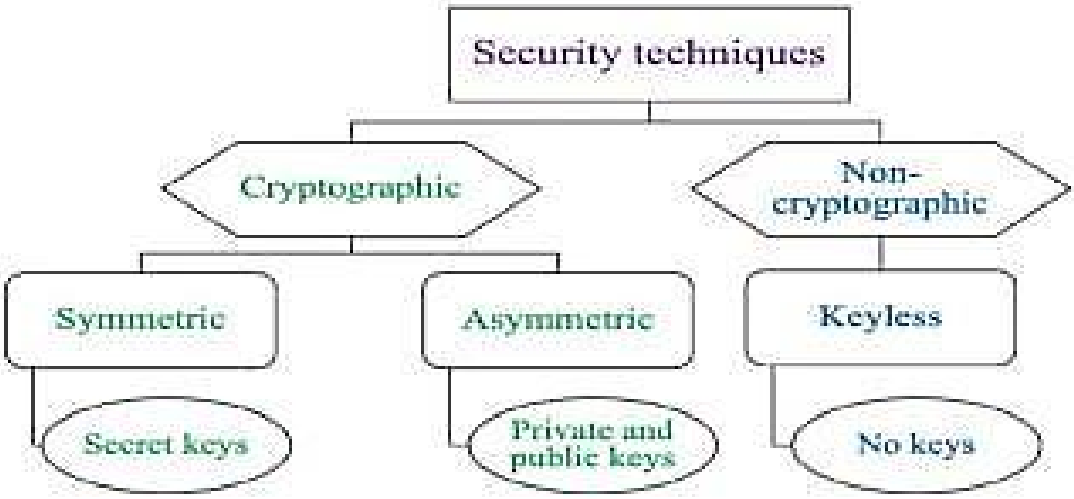


Figure 2.10: Security Techniques[31].

Symmetric-Key Algorithms

Symmetric cryptography comprises any cryptographic algorithm based on a secret/shared key between two or more nodes wanting to interconnect. The key is to be created and circulated prior to using asymmetric cryptography or a prior communication phase.

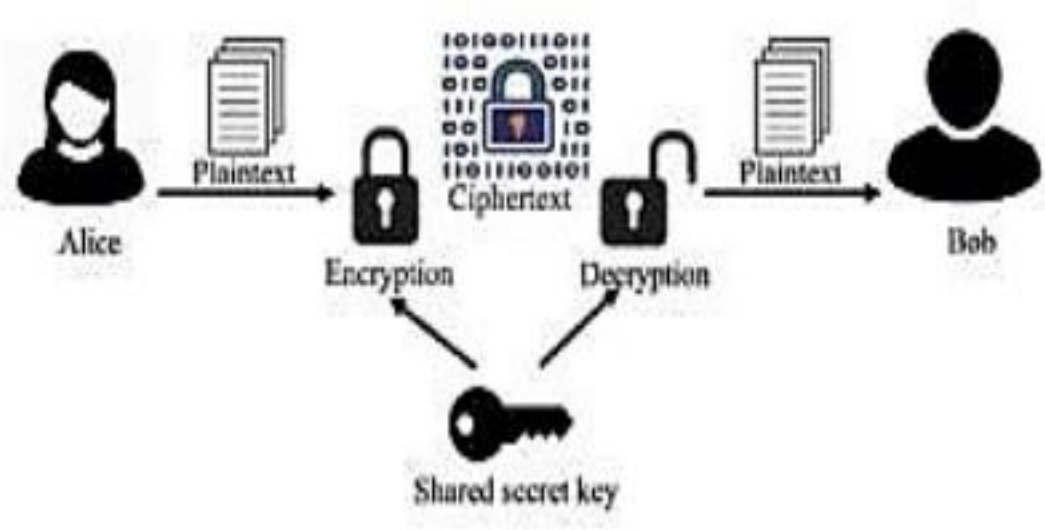


Figure 2.11: Symmetric Cryptography[32]

2.3 Challenges for IoT

There are three main tasks that still must be subjugated for IoT to be effective. The first task is a technical one. The interoperability of smart devices, the major feature of IoT, still needs to be worked out. All linked devices from various companies should operate effortlessly to be valued, this is also significant for the interchange of information. This will need open standards and industry-wide interoperability[33]. It's clear this will take some time, but in the words of a researcher:

"The industry knows how to do it; we did it for the first stage of the Internet and for the cloud. The current task at hand is even bigger and more complex, but I know that the IoT community is up for the challenge[33].

What are the challenges of IoT in healthcare?

1) Data Security and Privacy

One of the most significant challenges faced by IoT is Data Security and Privacy. IoT-enabled mobile devices capture data in real-time, but most of them lack adherence to data protocols and standards.

There is significant ambiguity regarding data ownership and regulation. Hence, the data stored within IoT-enabled devices are prone to data thefts and it makes the data more susceptible to cybercriminals that can hack into the system to compromise personal health information. Some examples of misuse of IoT device data are fraudulent health claims and the creation of fake IDs for buying and selling drugs.

2) Integration: Multiple Devices & Protocols

The integration of multiple types of devices causes hindrance in the implementation of IoT in the healthcare sector. The reason behind this hindrance is that device manufacturers haven't reached a consensus regarding communication protocol and standards. This results in a scenario where every manufacturer creates its own separate ecosystem of IoT devices that do not work with the devices and applications of competing manufacturers. In such a situation, there is no synchronous protocol that could be followed for data aggregation. This nonuniformity slows down the process and reduces the scope of scalability of IoT in healthcare.

3) Data Overload and Accuracy

Due to the non-uniformity of data and communication protocols, it is difficult to aggregate data for vital insights and analysis. IoT collects data in bulk and for proper data analysis, the data need to be segregated in chunks without overloading with precise accuracy for better results. Moreover, the overloading of data might affect the decision-making process in the hospitality sector in the longer run.

4) Cost

You might not be surprised to see this point here. Costs are one of the greater challenges when planning to consider IoT app development for healthcare mobility solutions. However, the costs are completely worth it if the IoT implementation is one that solves a genuine problem. While you will spend a significant amount of money and resources in developing an IoT application, the returns will be equally huge when your business saves time and manpower, all while improving the business processes, generating more revenue streams, and creating more business opportunities through IoT[43].

2.3.1 Problems of Use of Internet of Medical Things in Telemedicine

Despite all of the promises and health communication benefits that telemedicine is proficient to deliver, it also generates severe demands that hinder or impend its development and application in several ways. These four major problems are.

1. Licensing and Legal Issues in Telemedicine

The first problems which are connected in countless regards that legitimately hamper the advancement of telemedicine comprise concerns connected to regional licensing, legal liabilities, and institutional credentialing of doctors[102]. Regrettably, lots of these legitimate problems are still unrequited and unsettled within both the Nigeria health care and judicial structures. For instance, in regional medical dealings where automated equipment is employed for surgery or radiology, if there is an automated letdown or hiccup that consequences in injuring the patient, deciding on who is accountable for that mishap is arguable and can be a major headache for legal authorities.

Another important concern inherent in this situation is that these physicians who are handling and interacting with the patient are operational out of different regions. Because laws concerning telemedicine and health care authorization are exclusive in each region, legal obligation,

misconduct, and authority become grave troubles of concern for the legal, judicial, and medical organizations[103]. For example, in the occasion that an untested doctor situated in Arizona in the USA is tangibly operating on a patient and is engaged in a live telemedicine communication with a professional in New York whose supervision and direction flop the surgery and upshot in the patient's demise, the district attorney and legal officials in Arizona would find difficulty in putting responsibility and lawsuit on the party in New York. A problem like this one is a usual situation in which telemedicine offers some lawful and authorizing concerns. Nevertheless, as telemedicine and its connected technology develop, practicable resolutions (specifically, legal policies and adjustments) to these complications should be exposed and made accessible.

2. Challenges to Patients Privacy

This is another severe barrier to the advancement of telemedicine comprises problems connected to patient confidentiality. According to researches, because numerous persons (i.e., technicians, nurses, etc.) are commonly engaged in telemedicine communication, exposure of personal records to all parties concerned becomes a danger to the confidentiality of that patient. Furthermore, albeit medical specialists take the responsibility of sustaining their patients' confidential rights, the other supporting parties involved in the telemedicine interaction may not be held to the similar average[45]. As a consequence of this danger to patients' confidential rights, telemedicine has struggled to receive approval from the authorized and medical societies. Conversely, again, as time evolves and this concern is undertaken by the health and legal societies alike, resolutions should be found to remove confidentiality risks to patients.

Additionally, these resolutions should produce improved acceptance of telemedicine practices by all parties troubled and, equally, should lessen the fear and frequency of cracks to patient confidentiality laws. Conflict from medical insurance organizations the next upsetting and

possibly the most important[108] – hindrance that telemedicine faces in gaining adoption is the trouble of getting compensation for services from insurance organizations that stand against exceptional consultations, like the ones absent of face-to-face contact. For example, according to researchers, the U.S. Health Care Financing Administration, a national institution in control of major health insurance corporations, specifies that repayment for medical services is generally accessible only when direct bodily communication (a face-to-face appointment) is held.

On the other hand, this specification is not general and required of all states. There are some states that do not require this instant presence in health consultations, such as California, Texas, and Oklahoma. In addition, these states even go as far as authorizing such telemedicine services as suitable substitutes for face-to-face appointments if suggested by the attending practitioner(s)[108].

3. Limited Knowledge and Expertise in Telemedicine

The last concern to be addressed has to do with the limited knowledge and know-how in telemedicine as well as the necessity for improved and modified telemedicine schemes. In this regard, little knowledge presently exists among medical doctors on how to efficiently and practically employ numerous types of telemedicine. This scarcity of intuition into telemedicine, in consequence, obstructs the creativeness to explore more effective and efficient modalities of telemedicine applications. As a consequence, training medical doctors to study and accept this novel manner of achieving health services, through telemedicine, has become an important obstacle to application.

Exceptional proficiency is also essential before application of telemedicine can be permitted and render success to those involved. In this respect, an exceptional word, Telemedicine, was

formed to designate the essential abilities and qualifications physicians must have in order to perform this type of specified task. Telemedicine is a must in order to be a health communication professional concerning telemedicine. In specific, there is a three-phase procedure involved in such health communication aptitude. As such, Telemedicine comprises of:

i. Planning and establishing,

ii. Learning and use, and

iii. Formalizing routines.

Regrettably, accomplishing this level of proficiency could be regarded a main opposition to telemedicine application, because substantial teaching and finances are not always accessible resources to permit this type of campaign. To this end, in some medical situations where resources are inadequate, telemedicine may not be a realistic or inexpensive option.

In the following section, several systems of telemedicine are adversely disparaged in regards to their subtractive effects on doctor–patient interaction. In every of the procedures acknowledged, people are left to interact with computers and other systems of technology, all of which are absent or slight in bodily human contact and altercation. As argued, the social and communicative fundamentals to these telemedicine modalities desensitize, dissocialize, and depersonalize human conduct and interaction. In addition, it was urged for a cautious re-examination of whether telemedicine sincerely serves humankind in an optimistic and productive way.

2.3.2 Probable Resolutions to the Problems Affecting the Use of Telemedicine

In taking an anti-telemedicine position, the problems stated previously validate that telemedicine is far from flaws: legal and certifying concerns, patient confidentiality, compensational conflict from insurance corporations, and learning paucities in telemedicine[46]. Even though the capacity

to better care for patients and save lives has enhanced, the possibility and difficulty of health care also have improved significantly. This is reason telemedicine opponents should open their eyes and try to find resolutions to these problems. A few grassroots procedures to correcting these matters are rallying the medical and legal groups together in order to resolve these concerns and try to find out any means essential to defeat these disruptive fundamentals from meddling with telemedicine's advanced course[47].

In the meantime, researchers believe that lawyers can amend telemedicine laws to elucidate and categorize accountability guidelines with respect to regional surgical procedures (when the operation occurs in one region while a physician is situated in another state).

More significant, another drawback of resorting to telemedicine is that it is deducting and close to removing our community human interaction in health care surroundings. This worry urges health communication researchers to appraise the explicit communicative requirements that have been otherwise ignored in the writings on telemedicine. As we have perceived, the social and communicative rudiments to these telemedicine modalities degrade, dissocialize, and depersonalize human activities and communication. For instance, because telemedicine can take the system of interaction between distant users, e-mail is oftentimes adopted as a channel to carry out such discourse[48].

Regrettably, e-mail is suitable only for asynchronous interaction. The query arises as to whether medical equipment will increasingly substitute patient–doctor interaction. We contend that it should be only an accessory to health care specialists.

Establishing elementary understanding of what this medical technology can give rise to will assistance health communication researchers educate the telemedicine argument by turning exceptional intuitions into more suitable methods that will improve and civilize facilitated portals

of health interaction, thus presenting solutions and explanations for functioning health care interaction and delivery.

Grasping the influence on users and data exchange is a vital force in the implementation of telemedicine by contradictory factors. Available study to deliver reasonable explanations of the essential reasons for patient fulfilment or dissatisfaction with telemedicine and to examine communication concerns in any depth is still lacking. The notion is that future study on the use of telemedicine requirements to be more systematically rigorous to aid policymakers reach up-todate decisions about the germane use of this medical practice.

Another rational method to accomplish general telemedicine in our health care physicians could be targeting medical schools to integrate such training into their programs. Because telemedicine is becoming gradually popular in its use in the health care business, health communication specialists should develop strategies of approaching medical schools to encourage them to integrate courses into their programs that teach the scholars on the most generally used methods of telemedicine and the systems expected to be used in the future. To this end, scholars would study the most significant facets of telemedicine services and would, after receiving their certifications to practice, use these services in their everyday jobs.

2.4 Related Works

A study conducted by researchers to decide the opinion of health personnel in the health-care towards telemedicine application in a novel tertiary teaching hospital, an improved structured questionnaire using a potential postal survey was administered to a cross-section of health workers in Lagos State University Teaching Hospital (LASUTH) and Lagos State University College of Medicine (LASUCOM). Only 60.9 % of respondents were conversant with this novel evolving notion of telemedicine in the health care scheme[110]. Even though, 50 % of health

personnel had articulated worry about the moral and medico-legal contemplation of telemedicine training, this was notwithstanding of their socio-religious experience. The major reasons weighing in favor of readiness to use telehealth services were awareness of telehealth applications (28.1 %); perception of telehealth advantages (14.1 %), reduced obstacles to telehealth care amongst others. Most of the respondents alleged that telehealth would improve direct access to health care services (23.4 %), progress significance of care (14.1 %) among others. It is anticipated to deliver telemedicine to patients particularly for emergency and chronic medical circumstances.

Research to evaluate the Knowledge and Perception of Telemedicine and E-health by Some Nigerian Health Care Practitioners. In this research, 200 healthcare workers comprising doctors, nurses, laboratory scientists, pharmacists, senior nursing senior medical students and medical records officer's radiographers were respondents in the evaluation of their understanding and awareness using interviews and semi structured questionnaire. 83 (41.5 %) of the respondents had meagre understanding of telehealth and only 42 (21 %) were aware of the nation's projected telehealth program. 141 (70.5 %) will use telehealth services and 138 (69 %) will applaud its use to others. 134 (67 %) alleged it should be involved in the three-tier health system while 114 (57 %) supposed it should be a special program. 162 (81 %) of the respondents were optimistic about the significance and benefits of telehealth introduction to the Nigerian health scheme. This consequence emphasized the requirement for stake holder's wide confab and public education prior to the invention of government policy on telemedicine due to existing poor level of data. Moreover, there is requirement for man power improvement for this program which possesses the prospective of taking dedicated healthcare services to the otherwise unreached while also

improving the awareness and expertise of healthcare specialists in secluded locations through distance learning.

On the evaluation of telemedicine readiness in some selected states in Western Nigeria[111]. Considering some critical factors of e-Health readiness such as need change readiness, engagement readiness and structural readiness. The responses were analyzed statistically using descriptive analysis. The analysis was applied to determine the e-Health readiness status of health practitioners, public, patients and the mangers from the western part of Nigeria. The result of the general assessment of all samples shows that (i) health managers are not structurally ready, (ii) the public and patient fairly agreed but structural factor will be a constraint and (iii) the healthcare practitioners fairly agreed but structural, social influence, engagement will affect the successful adoption of the invention.

Research was carried out on the extent of telehealth use in rural and urban hospitals[116]. Data was gotten from 4,727 hospitals in the 2013 Healthcare Information and Management Systems Society (HIMSS) and their analysis yielded these findings: Two-thirds (66.0 % of rural and 68.0 % of urban) had no telehealth services or were only in the process of implementing a telehealth application. One-third (34.0 % rural and 32.0 % urban) had at least one telehealth application currently in use.

Among hospitals with "live and operational" telehealth services, 61.4 % indicated only a single department/program with an operational telehealth service, and 38.6 % indicated two or more departments/programs with operational telehealth services. Rural hospitals were significantly less likely to have multiple services (35.2 %) than were urban hospitals (42.1 %).

Rural and urban hospitals did not differ significantly in overall telehealth implementation rates but did differ in the department where telehealth was implemented. Urban hospitals were more

likely than rural hospitals to have operational telehealth implementations in cardiology/stroke/heart attack programs (7.4 % vs. 6.2 %), neurology (4.4 % vs. 2.1 %), and obstetrics/gynecology/NICU/pediatrics (3.8 % vs. 2.5 %). In contrast, rural hospitals were more likely than urban hospital to have operational telehealth implementations in radiology departments (17.7 % vs. 13.9 %) and in emergency/trauma care (8.8 % vs. 6.3 %)[115].

2.4.1 Hooshmand Theory of Cost Minimization

The theoretical framework for this study is based on the theoretical model of researcher, which has been further modified by other works, especially in the study that addressed the issue of cost from the perspective of the parents/guardians of children with special health care needs (CSHCN) when care is provided via telemedicine.

Families of CSHCN face financial burdens beyond that of families of healthy children. The cost framework for this study is a cost minimization analysis framework. Cost minimization is a form of a cost-effectiveness analysis which presumes the effectiveness or outcomes of a program are similar but that the costs are different

This framework focused on the difference in costs between the comparable interventions of traditional face-to-face care and telemedicine. This study focused on the cost difference from the perspectives of the family of the CSHCN, recognizing the importance of reducing financial burden and hardship for this vulnerable population[49].

Using the cost-minimization framework, the study examined cost from the family perspective comparing the costs of traditional face-to-face care to care provided utilizing telemedicine. This included both direct and indirect costs as well as hidden costs recognized by the family but not evident to those outside the family or community health providers. Costs examined included travel, lodging, loss of wages, child care, and ancillary family costs such as food. The Cost

framework was developed for this research project to measure both direct and indirect costs for the purpose of this research.

2.5 Summary of Literature Reviewed

From the review of Literature, Theoretical framework considered Hooshmand theory of Cost Minimization. The theory focused on the difference in costs between the comparable interventions of traditional face-to-face care and telemedicine. Using the cost-minimization framework, the study examined cost from the family perspective comparing the costs of traditional face-to-face care to care provided utilizing telemedicine.

The study was able to establish the concept of variables. It discussed the types of telemedicine to include: Tele cardiology, Tele dermatology, Tele radiology, Telepathology and Tele pharmacology. It also highlighted the effects of Telemedicine on medical service delivery, challenges against the use of telemedicine in medical services delivery as well as possible solutions to the identified challenges. Lack of professionals and unavailability of facilities are the major challenges against the use of Telemedicine identified from related literature reviewed.

Empirical studies relating to this work were reviewed such as perception of health workers in the health-care towards telemedicine application in Lagos State University Teaching Hospital (LASUTH) and Lagos State University College of Medicine (LASUCOM), Knowledge and Perception of Telemedicine and E-health by Some Nigerian Health Care Practitioners, assessment of telemedicine readiness in some selected states in Western Nigeria, extent of telehealth use in rural and urban hospitals. Through this study of literature, it was established that there is a need to review telemedicine policies and curricula of medical schools to help promote the use of telemedicine in medical services delivering. Thus, the next chapter will outline the

methodology in trying to evaluate the perceived effects of telemedicine in medical services delivery in Federal Medical Centers.

Endnotes

1. A. J. Onumanyi, A. M. Abu-Mahfouz & G. P. Hancke. *Low Power Wide Area Network, Cognitive Radio and the Internet of Things: Potentials for Integration.* **Sensors (Basel, Switzerland)**, 2020, 20(23), 6837. https://doi.org/10.3390/s20236837

2. S. Hamdan, M. Ayyash, & S.Almajali. *Edge-Computing Architectures for Internet of Things Applications: A Survey.* **Sensors (Basel, Switzerland)**, 2020, 20(22), 6441. https://doi.org/10.3390/s20226441
3. R. Fereira, C. Ranaweera, K. Lee & J.G Schneider. *Energy Efficient Node Selection in Edge-Fog-Cloud Layered IoT Architecture*. **Sensors (Basel, Switzerland)**,2023,23(13), 6039. https://doi.org/10.3390/s23136039

4. S.D. Mamdiwar, Z. Shakruwala, U. Chadha, K.Srinivasan, & C.Y Chang. *Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring.* **Biosensors**, 2021, 11(10), 372. https://doi.org/10.3390/bios11100372

5. M. Aledhari, R. Razzak, B. Qolomany, A. Al-Fuqaha, & F. Saeed. *Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions.* **IEEE access: practical innovations, open solutions**, 2022 10, 31306–31339. https://doi.org/10.1109/ACCESS.2022.3159235

6. Varistor. (N.D.). The Advantages And Disadvantages Of Internet Of Things.

7. S. Roy, & D. Sarddar. *The Role of Cloud of Things in Smart Cities*. **International Journal of Computer Science and Information Security (IJCSIS)**, 2016,14.

8. Gao, W., et al. "Telemedicine Systems and IoMT Interoperability for Remote Healthcare." *Journal of Healthcare Informatics Research*, 2023, 7(1), 45-58. doi:10.1007/s41666-023-00230-5.
9. S. Senthilkumar, Poorana, & B. Subramani. *Study on IoT Architecture, Application Protocol and Energy needs.* **Biosensors**, 2020, 8, 7-12.

10. S. Ajami, & A. Rajabzadeh. Radio Frequency Identification (RFID) technology and patient safety. **Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences**, 2013,18(9), 809-813.

11. N. Garcia. *The Internet Protocol -- Past, some current limitations and a glimpse of a possible future.* 2021.

12. Balogun, A. O., et al. "AI-Powered IoMT for Enhancing Interoperability in Telehealth Systems." *Journal of Telemedicine and Telecare*, 2024, 30(2), 101-112. doi:10.1177/1357633X23108419.

13. C. Nwabueze, M. Eng, M.Silas, & S. Akaneme. *Wireless fidelity (Wi-Fi) broadband network technology: An overview with other broadband wireless networks*. **Journal of Technology in Human Services**, 2023, 28(1), 71-78.

14. I.S. Faustov, & A.B. Tokarev. *Address direction finding of ZigBee devices*. **Radio engineering,** 2023, 8. https://doi.org/10.18127/j00338486-202308-13

15. A. Coboi, M. Nguyen, P. Van Nam, T. Chien, M. Nguyen, & D. Nguyen. *Zigbee based mobile sensing for wireless sensor networks*. **Journal of Wireless Sensor Networks**, 2023,1, 325–342. https://doi.org/10.37256/1220233923

16. A. Coboi, V.C. Nguyen, M. Nguyen, N. Duy, & T. Tran. *An analysis of ZigBee technologies for data routing in wireless sensor networks*. **Journal of Wireless Sensor Networks**, 2021.

17. N. Singh. *Near-field communication (NFC)*. **Information Technology and Libraries**, 2020,39. doi:10.6017/ital.v39i2.11811

18. A. Singh, A. Luhach, X.Z. Gao, S. Kumar, & D. Sinha Roy. *Evolution of wireless sensor network design from technology centric to user centric: An architectural perspective.* **International Journal of Distributed Sensor Networks**, 2020, 16, 1550147720949138. doi:10.1177/1550147720949138

19. M. Ansari, S. Ali, & M. Alam. *Internet of things (IoT) fusion with cloud computing: current research and future direction.* **International Journal of Advanced Trends in Electrical and Electronics Engineering**, 2023, 9, 1812-1845. https://doi.org/10.19101/IJATEE.2021.876002.

20. J. Kissi, S. Dogbe, J. Banahene, O. Ernest, & B. Dai. Predictive factors of physicians' satisfaction with telemedicine services acceptance. 2020, https://doi.org/10.1177/1460458219892162

21. T. Shakeel, S. Habib, W. Boulila, A. Koubaa, A.R. Javed, M. Rizwan, T. Gadekallu, & M. Sufiyan. *A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects.* **Complex & Intelligent Systems**, 2022, 9. https://doi.org/10.1007/s40747-022-00767-w

22. Zhang, S., et al. "IoMT Interoperability in Pediatric Telemedicine: An Overview of Current Advances." *IEEE Access*, 2023, 11, 21256-21268. doi:10.1109/ACCESS.2023.3261210.

23. A. Kotha & K. Manohar. *A device-based interoperability as a service for IoMT devices*. **Journal of Ambient Intelligence and Humanized Computing**, 2023,14, 1-12. https://doi.org/10.1007/s12652-023-04669-8

24. Sahalu, Y., et al. "FHIR and IoMT Interoperability for Remote Patient Monitoring." *Healthcare Informatics Research*, 2021, 27(3), 187-196. doi:10.4258/hir.2021.27.3.187.

25. M. Patra, B. Sahoo, & A. Turuk. *Smart Healthcare System Using Containerized Internet of Medical Things.* **In Handbook of Research on Smart Computing for Healthcare and Medicine,** 2022(pp. 18). doi:10.4018/978-1-6684-4580-8.ch014

26. P. K. Sadhu (Central Michigan University). *Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions*. **Sensors**, 2022, 22(15), Article 5517. https://doi.org/10.3390/s22155517

27. A. Ghubaish, T. Salman, M. Zolanvari, & D. Unal. *Recent Advances in the Internet of Medical Things (IoMT) Systems Security.* **IEEE Access**, 2020 8, 147692-147708. https://doi.org/10.1109/ACCESS.2020.3019819

28. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, & R. Jain. *Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security*. **IEEE Internet of Things Journal**, 2021, 8(11), 8707-8718. DOI: 10.1109/JIOT.2020.3045653

29. Y. Khan, M. Bin Mohd Su'ud, M.P. Alam, & S.F. Ahmad. *Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications.* **Electronics**, 2022, 12(1), 88. DOI: 10.3390/electronics12010088.

30. J. Lim. *Scalable Fog Computing Orchestration for Reliable Cloud Task Scheduling*. **Applied Sciences**, 2021,11(22), 10996. DOI: 10.3390/app112210996.

31. A. Onesimu, J. Karthikeyan, & Y. Sei. *An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT-based healthcare services*. **Peer-to-Peer Networking and Applications**, 2021 14(15). DOI: 10.1007/s12083-021-01077-7.

32. L. Hu, C. Xiang & C. Qi. *Research on Traceability of Cold Chain Logistics Based on RFID and EPC.* **IOP Conference Series: Materials Science and Engineering,** 2020 790, 012167. doi:10.1088/1757-899X/790/1/012167

33. A. Dutta. *Application of Barcode Technology in Library: Planning and implementation*. **Journal Name**, 2022, 7, 40-44.

34. N. Arinze, G.N. ONOH, & D. Abonyi. *Performance of Light Fidelity and Wireless Fidelity Networks in a WLAN.* **International Journal of Research in Engineering & Science**, 2020, 4. doi:10.26808/rs.re. v4i1.02

35. Mahesh, V., et al. "IoMT-Enabled Telemedicine Platforms: Ensuring Interoperability and Data Integrity." *Journal of Telemedicine and Telecare*, 2023, 29(3), 145-158. doi:10.1177/1357633X22109789.

36. S. Shrestha, & S. Shakya. *Technical Analysis of ZigBee Wireless Communication.* **Journal of Trends in Computer Science and Smart Technology**, 2021, 2, 197-203. doi:10.36548/jtcsst.2020.4.004

37. S. Dandi. *Study of ZIGBEE Technology and its Application in Wireless Automation System.* **International Journal of Trend in Scientific Research and Development (IJTSRD)**, 2020, 4(2), 1003-1006. Retrieved from https://www.ijtsrd.com/papers/ijtsrd30200.pdf

38. G. Mehmood, M. Khan, A. Waheed, M. Zareei, M. Fayaz, T. Sadad, N. Kama, & A. Azmi. *An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network.* **Complexity**,2021. https://doi.org/10.1155/2021/6577492

39. S. Albouq, A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti, & N. Bahbouh. *A Survey of Interoperability Challenges and Solutions for Dealing with Them in IoT Environment.* **IEEE Access**, 2022,10, 1-1. https://doi.org/10.1109/ACCESS.2022.3162219

40. R. Solimini, F. Busardò, F. Gibelli, A. Sirignano, & G. Ricci. *Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic.* **Medicina (Kaunas, Lithuania)**, 2021, 57. https://doi.org/10.3390/medicina57121314

41. P. G R, R. Hegde, B. K B, T. Jan, & G. Naik. *Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges*. **IEEE Access**, PP,2024. https://doi.org/10.1109/ACCESS.2024.3362239

42. S. Rahi, M. Munawar Khan, & M. Alghizzawi. *Factors influencing the adoption of telemedicine health services during COVID-19 pandemic crisis: An integrative research model*. **Enterprise Information Systems,** 2020. https://doi.org/10.1080/17517575.2020.1850872

43. T. Ghiwaa, I. Khan, M. White, & N. Beloff. *Telemedicine Adoption for Healthcare Delivery: A Systematic Review*. **International Journal of Advanced Computer Science and Applications**, 2023,14. https://doi.org/10.14569/IJACSA.2023.01411125

44. A. A. Mubaraki, A. D. Alrabie, A.K. Sibyani, R. S. Aljuaid, A. S. Bajaber, & M. A. Mubaraki. *Advantages and disadvantages of telemedicine during the COVID-19 pandemic era among physicians in Taif, Saudi Arabia*. **Saudi medical journal**, 2021, 42(1), 110–115. https://doi.org/10.15537/smj.2021.1.25610

45. T. Gruzdeva, E. Rentsen, & T. Natsagdorj. *Fractional programming approach to a cost minimization problem in electricity market.* **Yugoslav Journal of Operations Research**, 2018, 29, 3-3. https://doi.org/10.2298/YJOR171115003G

46. S. Khezr, M. Moniruzzaman, A. Yassine, & R. Benlamri. *Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research*. **Applied Sciences**, 2021, 9(9), 1736. https://doi.org/10.3390/app9091736

47. M. Seth, H. Jalo, A. Högstedt, O. Medin, U. Björner, B.A. Sjöqvist, & S. Candefjord. *Technologies for Interoperable Internet of Medical Things Platforms to Manage Medical Emergencies in Home and Prehospital Care: Protocol for a Scoping Review.* **JMIR research protocols**, 2022,11(9), e40243. https://doi.org/10.2196/40243

48. M. Shafiq, J.G. Choi, O. Cheikhrouhou, & H. Hamam. Advances in IoMT for Healthcare Systems. **Sensors (Basel, Switzerland)**, 2023, 24(1), 10. https://doi.org/10.3390/s24010010

49. I. Villanueva-Miranda, H. Nazeran, & R. Martinek. *A Semantic Interoperability Approach to Heterogeneous Internet of Medical Things (IoMT)* Platforms. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-5). **Ostrava, Czech Republic**, 2018. doi:10.1109/HealthCom.2018.8531103

50. A. Muhammad Auwal. ***IoT Integration in Telemedicine: Investigating the Role of Internet of Things Devices in Facilitating Remote Patient Monitoring and Data Transmission***, 2023. doi:10.21203/rs.3.rs-3419693/v1

51. L. Alashlam, & A. Alzubi. Taxonomic Exploration of Healthcare IoT: Challenges, Solutions, and Future Frontiers. **Applied Sciences,** 2023, 13(22), 12135. https://doi.org/10.3390/app132212135

52. S. S. Albouq, A. A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti, & N.M. Bahbouh. A *Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment*. **IEEE Access**, 2022,10.1109/ACCESS.2022.3162219.

53. D. Dione, I. Diop, I. Gueye, B. Ngom, & S. Farssi. *Proposal for an IoT-based e-health model in developing countries: Case of Senegal*, **International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa**, 1-7, 2021. doi:10.1109/ICECET52533.2021.9698664

54. Abdulkadir, B. A., et al. "Overcoming Interoperability Barriers in IoMT with AI: A Review." *Journal of Telemedicine and Telecare*, 2022, 28(5), 332-344. doi:10.1177/1357633X21106989.

55. J. T. Kelly, K.L. Campbell, E. Gong, & P. Scuffham. *The Internet of Things: Impact and Implications for Health Care Delivery.* **Journal of medical Internet research**, 2020, 22(11), e20135. https://doi.org/10.2196/20135

56. M.O. Edeh, E.E. Otto, N.E. Richard-Nnabu, S.G. Ugboaja, C.C. Umoke, & D. Omachi. *Potential of Internet of Things and Semantic Web Technologies in the Health Sector*. **Nigerian Journal of Biotechnology**, 38(2), 73-83. doi: https://dx.doi.org/10.4314/njb.v38i2.8

57. R. Gupta. *Research Paper on Artificial Intelligence*. **International Journal of Engineering and Computer Science**, 2023, 12(2), 25654-20656. doi:10.18535/ijecs/v12i02.4720

58. Iqbal, T., & Sheikh, A. "IoMT in Pandemic Response: Telemedicine Integration and Interoperability Challenges." *IEEE Access*, 2021, 9, 47268-47279. doi:10.1109/ACCESS.2021.3066259.

59. M.A. Rahman, E. Victoros, J. Ernest, R. Davis, Y. Shanjana, & M.R. Islam. *Impact of Artificial Intelligence (AI) Technology in Healthcare Sector: A Critical Evaluation of Both Sides of the Coin*. **Clinical pathology (Thousand Oaks, Ventura County, Calif.)**, 2024, 17, 2632010X241226887. https://doi.org/10.1177/2632010X241226887

60. A. Ramalingam, A. karunamurthy, Dr, & B. Pavithra. *Impact of Artificial Intelligence on Healthcare: A Review of Current Applications and Future Possibilities*. **Quing International Journal of Innovative Research in Science and Engineering**, 2023, 2(2), 37-49. doi:10.54368/qijirse.2.2.0005

61. S. Singla. AI and IoT in Healthcare. *In Advances in Artificial Intelligence,* **Indian Conference on Artificial Intelligence, ICAI 2020, Goa, India, January 16–19**, 2023, 2020, Proceedings (pp. 1-23). doi:10.1007/978-3-030-37526-3_1

62. H. Chang, J.Y. Choi, J. Shim, M. Kim, & M. Choi. *Benefits of Information Technology in Healthcare: Artificial Intelligence*, **Internet of Things, and Personal Health Records.** 2023, 29(4), 323–333. https://doi.org/10.4258/hir.2023.29.4.323

63. A. Aldwean, & D. Tenney. *Artificial Intelligence in Healthcare Sector: A Literature Review of the Adoption Challenges.* **Open Journal of Business and Management**, 2024, 12(1), 1-9. doi:10.4236/ojbm.2024.121009

64. K. Naqvi, E. Markus, M. Muthoni, & A. Abu-Mahfouz. *A Critical Review of IoT-Connected Healthcare and Information Security in South Africa*. **In Advances in IoT, Industrial Informatics and Smart Applications**, 2022, (pp. 739-746). doi:10.1007/978-981-16-4016-2_70

65. A. Alemnji Ngufor. *The Role of Big Data in Healthcare: The Revolution of African Healthcare.* **African Journal of Health Sciences**, 2021, 1, 43-53.

66. R. Gwala, & P. Mashau. *Digitalisation of Healthcare and the Fourth and Fifth Industrial Revolutions in Africa.* **In Handbook of Research on Fourth and Fifth Industrial Revolutions in Africa**, 2024, (pp. 231-258). doi:10.4018/979-8-3693-0928-5.ch008

67. M. Alenezi, H. Alabdulrazzaq, & N. Mohammad. *Symmetric Encryption Algorithms: Review and Evaluation Study*. **International Journal of Communication Networks and Information Security**, 2020, 12, 256.

68. M. Ubaidullah, & Q. Makki. *A Review on Symmetric Key Encryption Techniques in Cryptography*. **International Journal of Computer Applications**, 2016, 147, 43-48. https://api.semanticscholar.org/CorpusID:64450272

69. R. Hireche, H. Mansouri, & A.S. Pathan. *Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis.* **Journal of Cybersecurity and Privacy**, 2022, 2, 640-661. doi:10.3390/jcp2030033

70. S.A. Wagan, J. Koo, I.F. Siddiqui, M. Attique, D.R. Shin, & N.M.F Qureshi. *Internet of medical things and trending converged technologies: A comprehensive review on real-time applications*. **Journal of King Saud University - Computer and Information Sciences**, 2022 34(10), 9228-9251.

71. S.S. Hameed, W.H. Hassan, L. Abdul Latiff, & F. Ghabban. *A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches*. **Peer Journal Computer science**, 2021, 7, e414. https://doi.org/10.7717/peerj-cs.414

72. H. Taherdoost. *Security and Internet of Things: Benefits, Challenges, and Future Perspectives*. **Electronics**, 2023, 12(8), 1901. https://doi.org/10.3390/electronics12081901

Chapter Three
Methodology

3.1 Architectural Design

In this section, we will provide an in-depth analysis of the architectural design of the Interoperability solution for IoMT in Telemedicine, based on the conceptual design.

3.1.1 Conceptual Diagram of The Interoperability Solution

A conceptual diagram provides a high-level representation of the structure and interactions within a system, illustrating how various components connect and work together to achieve interoperability, without focusing on technical specifics. It serves as a blueprint to help visualize the flow of data and the roles of each part in the system, making complex processes easier to understand.

Figure 3.1 presents a conceptual diagram of the interoperability framework within a healthcare system, integrating IoMT (Internet of Medical Things), cloud computing, and APIs to deliver data and services to end-user applications like hospital management, telemedicine, and machine learning.

1. **IoMT Layer**:
    - This layer encompasses various medical and health-related IoT devices, starting with **Device Sensors** that collect data from medical equipment and patient monitoring systems.
    - **Data Format Management** ensures the collected data is standardized, making it compatible for transmission and integration across platforms.

- **IoMT Data Security** safeguards sensitive health data by implementing encryption, authentication, and compliance measures.
- **IoMT Gateway** acts as a bridge, securely transmitting data from the IoMT layer to the cloud.

2. **API Layer**:
    - **Data Transfer between IoMT and Integrations** serves as a central API channel, facilitating the secure and standardized exchange of data between IoMT devices and the cloud infrastructure.
3. **Cloud Computing Layer**:
    - **Business Layer** processes high-level business logic, such as user management, billing, and analytics.
    - **Application Layer** handles application-specific processes and services that manage user interactions, data processing, and workflows.
    - **Data Format Layer** ensures incoming data from various sources is correctly formatted and normalized.
    - **Security Layer** provides robust protection for data in transit and at rest within the cloud, ensuring privacy and integrity.
4. **Consumer API Layer**:
    - This API layer acts as an intermediary between the cloud and end-users, allowing different applications to access and interact with the system.

5. **End Users**:

- The system supports multiple end-user applications, such as Hospital Management systems, Telemedicine platforms, and Machine Learning applications, each utilizing data and functionalities provided through the interoperability architecture.

This model demonstrates a seamless data flow from IoMT devices to cloud-based applications, ensuring that various healthcare and analytical applications can interact with and utilize data securely and effectively.

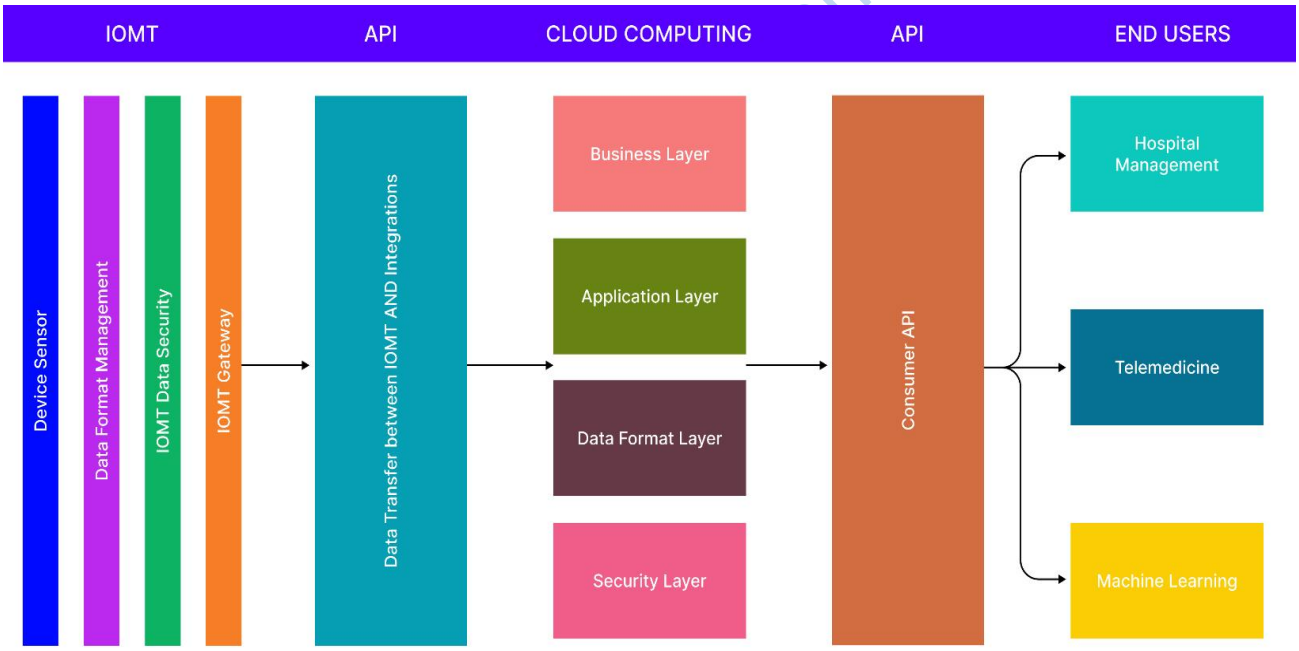


Figure 3.1: Conceptual Diagram of Interoperability in a Telemedicine (Source: Researcher, Olayinka W. 2024)

3.1.2.1 IoMT Architecture

The architectural design of the proposed solution is structured to seamlessly integrate IoMT devices with a telemedicine framework. This section provides a comprehensive overview of the key components and their interactions within the IoMT architecture as shown in the diagram.

3.1.2.2 IoMT Mobile Application

The core of the architecture lies in the IoMT mobile application, which consists of three fundamental layers.

Device Sensors

This layer is responsible for direct data collection using Software Development Kit (SDK) commands. The implementation ensures efficient and accurate acquisition of data from various sensors integrated into IoMT devices.

Data Format Management

The Data Format Management layer encapsulates commands and configures endpoints for the seamless interaction between sensors and the subsequent layers. This ensures the standardized formatting of data for further processing.

Gateway

Managing the connectivity of IoMT devices to the network, the Gateway layer ensures robust and secure communication. It plays a pivotal role in facilitating the flow of data between the IoMT mobile application and the broader network infrastructure.

1. **Program**:

- The entry point of the system where the Main function resides. This method (Main(string[] args) : async) likely initializes the system and coordinates interactions among the components.
- It uses the IoMTGateway and AuthenticationManager to manage connections and authenticate access.

2. **IoMTDevice**:
   - Represents an IoMT device with a deviceId attribute.
   - The method sendData(string data) is used to send data from the device through the IoMTGateway.
3. **IoMTGateway**:
   - Serves as the communication hub for IoT devices, responsible for managing connections and data flow between the IoMT devices and other components.
   - Properties include brokerAddress, port, username, and password for setting up the connection.
   - Methods:
     - SubscribeToTopicAsync(string topic): Allows the system to subscribe to specific data topics.
     - PublishMessagesAsync(string topic, string message): Publishes messages to a specified topic.
   - This gateway also handles authentication through the AuthenticationManager and data encryption via the EncryptionService.

4. **AuthenticationManager**:
    - Manages user authentication, providing methods to authenticate users with a username and password (AuthenticateUser(string username, string password)) or a certificate (AuthenticateWithCertificate(Certificate cert)).
    - It relies on the Certificate component for validating certificates as part of the authentication process.
5. **Certificate**:
    - Holds certificate data (string certificateData) and a method validate() to verify the authenticity of a certificate. This validation is used in conjunction with AuthenticationManager to secure the system.
6. **DataStorage**:
    - Responsible for storing and retrieving encrypted data.
    - Methods:
        - StorageData(string encryptedData): Stores encrypted data.
        - RetrieveData(string dataId): Retrieves data by its ID.
    - This component ensures that data at rest remains secure.
7. **EncryptionService**:
    - Provides encryption and decryption services for data before it's stored or sent across the system.
    - Methods:
        - EncryptData(string data): Encrypts data to secure it.
        - DecryptData(string encryptedData): Decrypts data when needed for processing.

- The IoMTGateway uses EncryptionService to secure data, and DataStorage relies on it to ensure stored data is encrypted.

Data Flow and Interactions

- The **Program** initializes and uses the **IoMTGateway** for device communication and **AuthenticationManager** for security.
- **IoMTDevice** sends data through the **IoMTGateway**, which authenticates users/devices using the **AuthenticationManager** and may validate certificates via **Certificate**.
- Data sent or stored is encrypted and decrypted by **EncryptionService** to ensure confidentiality and integrity.
- **DataStorage** handles encrypted data storage and retrieval, securing data at rest.

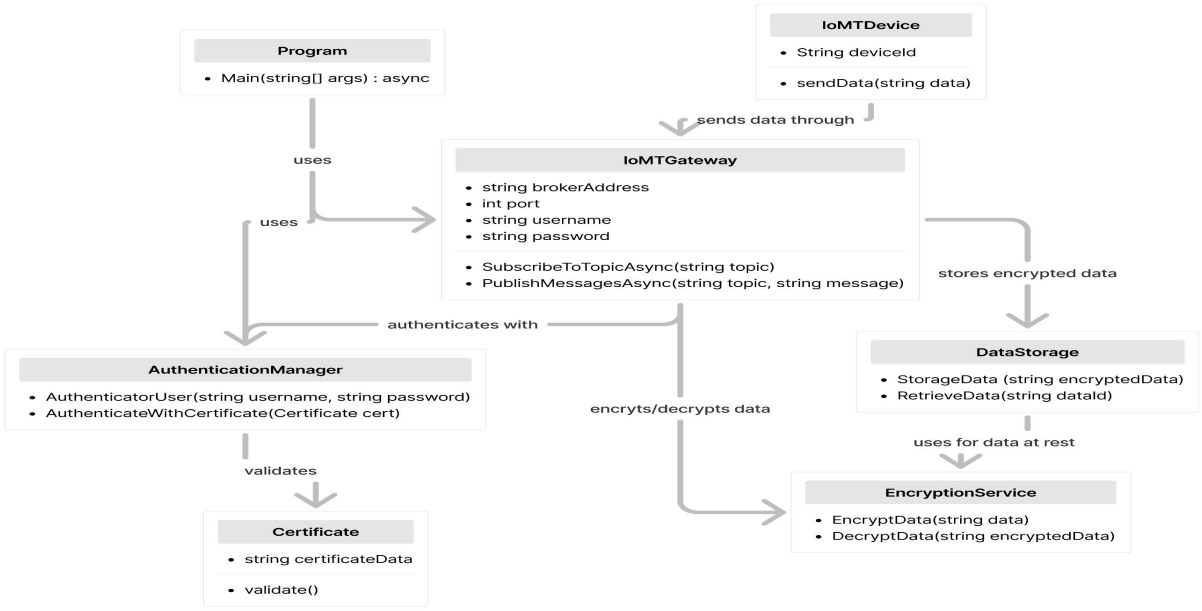


Figure 3.2: IoMT Gateway Architecture for Secure Data Transmission (Source: Researcher, Olayinka W., 2024)

3.1.1.2 API

Facilitating the exchange of data between the IoMT mobile application and the Cloud Application, the API layer serves as a bridge between the device and the centralized processing unit.

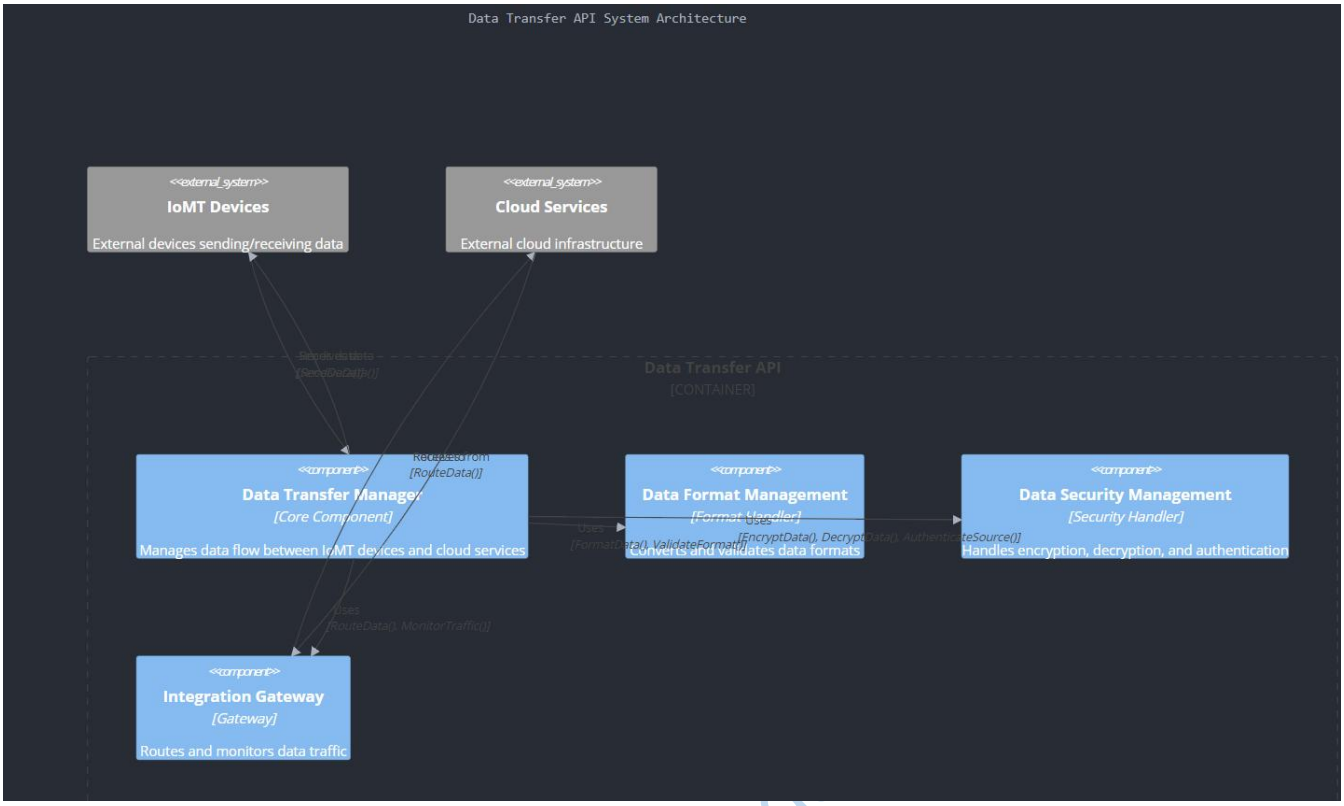


Figure 3.3: Researcher's Computation, 2024

3.1.1.3 Cloud Computing

This layer is the processing hub where data from the API is analyzed, processed, and stored. The The Cloud Computing component diagram in Figure X illustrates the layered structure within a cloud-based system. This structure acts as a processing hub where data from various sources, such as APIs, is received, processed, analysed, and stored. The diagram consists of four main layers, each responsible for specific aspects of data management and functionality within a cloud environment.

- **Security Layer**: This top layer ensures data integrity and secure access by implementing security protocols and managing user authentication and authorization.

- **Application Layer**: It handles user interaction and application services, including an API Gateway for managing external API requests. This layer facilitates communication between the user interface and the core business logic.
- **Business Logic Layer**: This layer is the core processing unit of the cloud system. It executes business rules and logic, validating data and ensuring compliance with operational policies.
- **Data Format Layer**: Responsible for data formatting and transformation, this layer manages data storage structure and standardization for seamless data retrieval and processing.

This architecture enables efficient data exchange, storage, and retrieval in cloud-based IoMT (Internet of Medical Things) applications, enhancing system functionality and security.

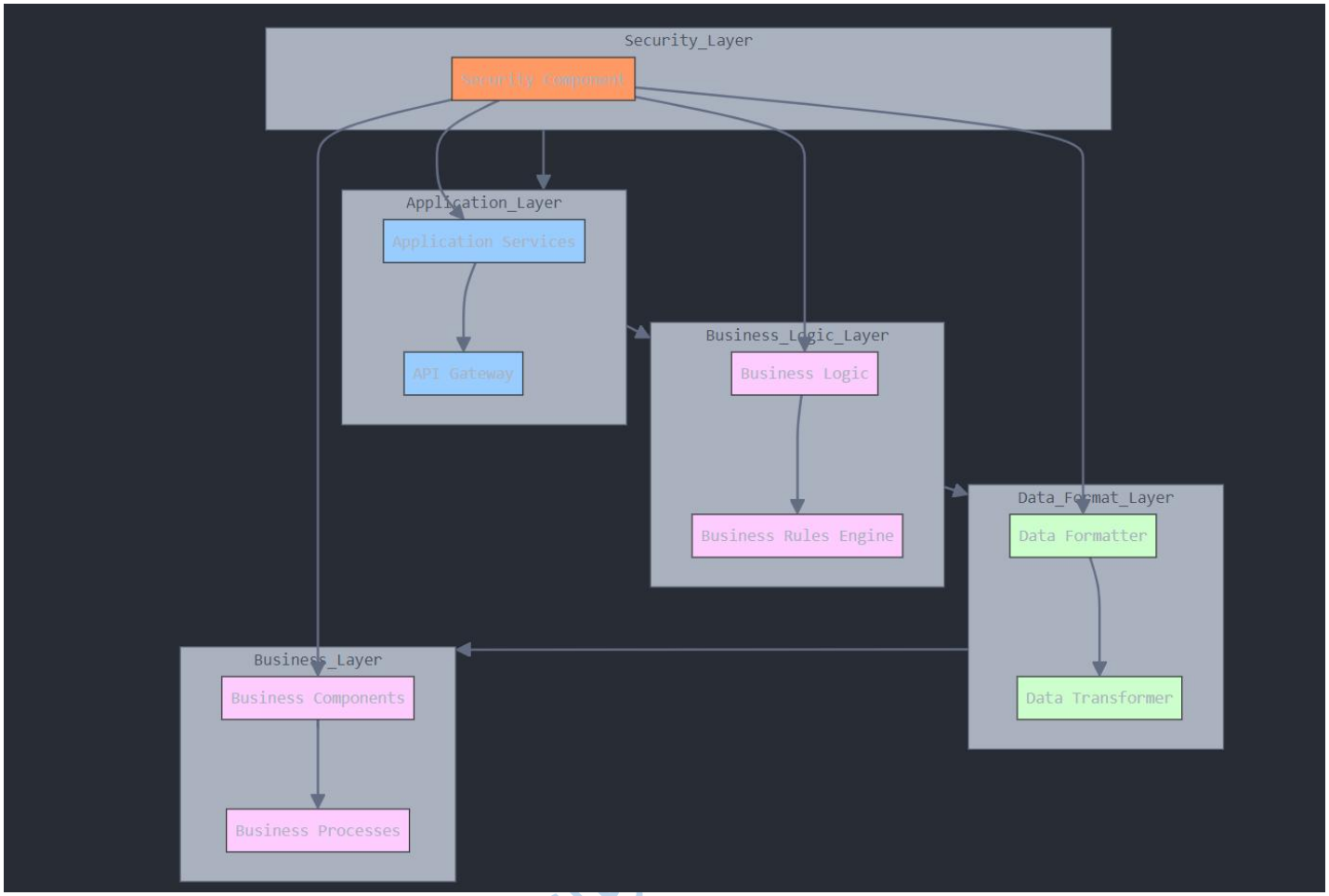


Figure 3.4: Component Diagram of a Cloud Computing System (Source: Researcher, Olayinka W. 2024)

3.2 Implementation

3.2.1 Development Environment Setup

The development environment was configured to support the tools and frameworks selected during the design phase. This included setting up integrated development environments (IDEs), version control systems, and necessary libraries. The specific tools used can be found in **Appendix A**.

3.2.2 Programming Languages and Tools

The implementation utilized specific programming languages and tools tailored to the requirements of the interoperability solution. A detailed list of the programming languages and tools employed in this project can be found in **Appendix B**.

3.2.3 API Development

RESTful APIs were developed to enable communication between systems. Each API was designed with carefully constructed endpoints and methods to ensure secure data transmission.

3.2.4 Middleware Solutions

Middleware tools were employed to facilitate communication between applications that utilize different protocols or data formats, ensuring a smooth data flow across the architecture.

3.2.5 Data Mapping and Transformation

A systematic approach was applied for data mapping and transformation, allowing data from various sources to be interpreted consistently within the interoperability framework.

3.2.6 Database Design

To ensure efficient data management, a carefully designed database is integrated into the Cloud Computing layer. This sub-section delves into the specifics of the database design, outlining its structure and relationships.

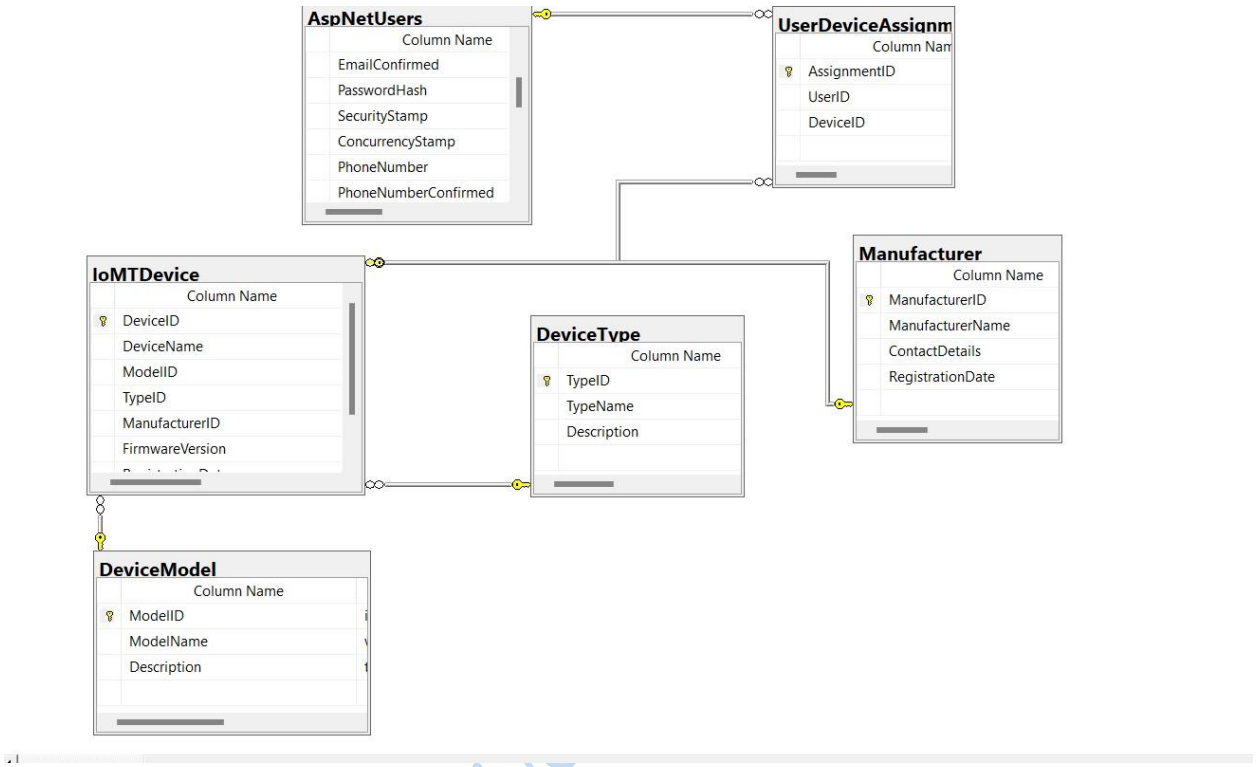


Figure 3.1: Entity Relationship Diagram (Source: Researcher, Olayinka W. 2024)

3.2.7 Telemedicine API

To establish a seamless connection between the IoMT ecosystem and *telemedicine applications, the Telemedicine API serves as a crucial interface, enabling the exchange of processed data.

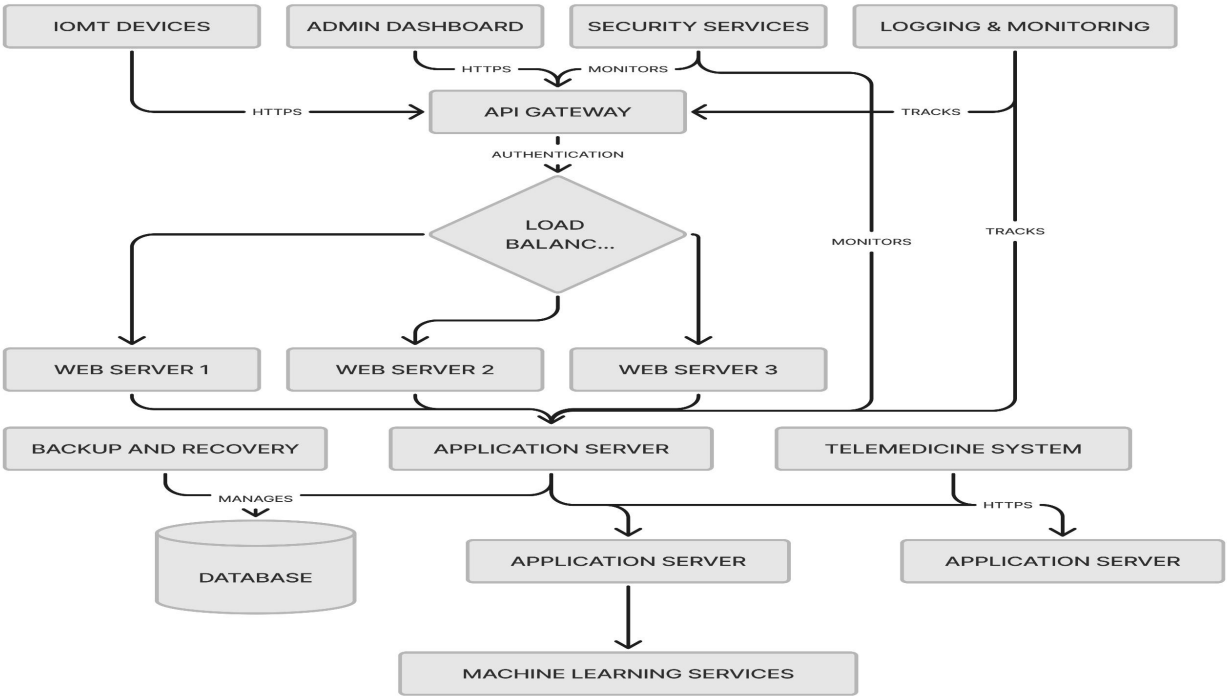


Figure 3.2: Interoperability API for Telemedicine Integration (Source: Researcher, Olayinka W. 2024)

3.2.8 Design Rationale

This subsection provides a rationale for the chosen architectural design, emphasizing how each component contributes to achieving the overarching goals of interoperability and efficiency in telemedicine.

Alignment with Project Objectives

The architectural design was meticulously crafted to align with the overarching objectives of the project, namely the development of an Interoperability solution for IoMT in Telemedicine.

Each architectural component was designed with a clear purpose, contributing directly to achieving the project's goals of seamless data exchange, efficiency, and integration with telemedicine applications.

Efficiency and Optimization

The design rationale emphasizes the efficiency gained through the proposed architecture. Each layer was carefully designed to optimize processes, ensuring swift and accurate data flow from device sensors to the telemedicine applications.

Discuss how the chosen architecture minimizes redundancy, latency, and resource consumption, leading to an overall improvement in system performance.

Scalability and Adaptability

Scalability is a key consideration in the design rationale, addressing the potential growth of the IoMT ecosystem and the increasing demands of telemedicine applications.

Highlight the flexibility embedded in the architecture to adapt to evolving technologies and future expansion, ensuring the longevity and relevance of the solution.

Interoperability Standards Compliance

The design rationale underscores the adherence to industry-standard interoperability protocols, emphasizing compatibility with existing and future IoMT devices and telemedicine applications.

Discuss how compliance with these standards enhances the solution's interoperability, enabling seamless integration into broader healthcare systems.

Security Measures

Security is a paramount concern, and the design rationale justifies the incorporation of robust security measures at various levels of the architecture.

Clearly outline how each layer contributes to data confidentiality, integrity, and access control, mitigating potential risks associated with sensitive health information.

User Experience Considerations

Considerations for a positive user experience are integrated into the design rationale. The architecture ensures that end-users, including healthcare professionals and patients, can interact with the IoMT solution seamlessly.

Discuss how the design choices contribute to user-friendly interfaces, intuitive workflows, and overall satisfaction.

Feedback from Existing Solutions

Drawing insights from prior IoMT and telemedicine solutions, we aim to incorporate valuable feedback and lessons learned into our design. The design rationale underscores how the proposed architecture strategically addresses and enhances areas where previous implementations faced challenges. Specifically, we focus on mitigating limitations observed in the selected IoMT ecosystem, recognizing that one major drawback has been the confinement of functionality to specific components within the IoMT landscape.

3.2.3 Scalability and Flexibility

An assessment of the architectural design's scalability and flexibility is essential. This section discusses how the proposed solution accommodates growth, technological advancements, and evolving healthcare needs.

3.2.4 Security Measures

To ensure the confidentiality and integrity of patient data, robust security measures are implemented. This sub-section outlines the security protocols embedded in each architectural layer.

3.2.5 Interoperability Standards

The IoMT architecture adheres to industry-standard interoperability protocols. This part discusses the standards adopted and how they contribute to seamless data exchange between different components.

This comprehensive exploration of the architectural design sets the foundation for subsequent chapters, providing a clear understanding of the system's structure and functionality.

3.3 Design

This section details the practical aspects of translating the architectural design into a functional Interoperability solution for IoMT in Telemedicine. It encompasses the development environment, IoMT mobile application implementation, API, Cloud Computing, and the associated database design. Below is the data flow diagram in the proposed architecture

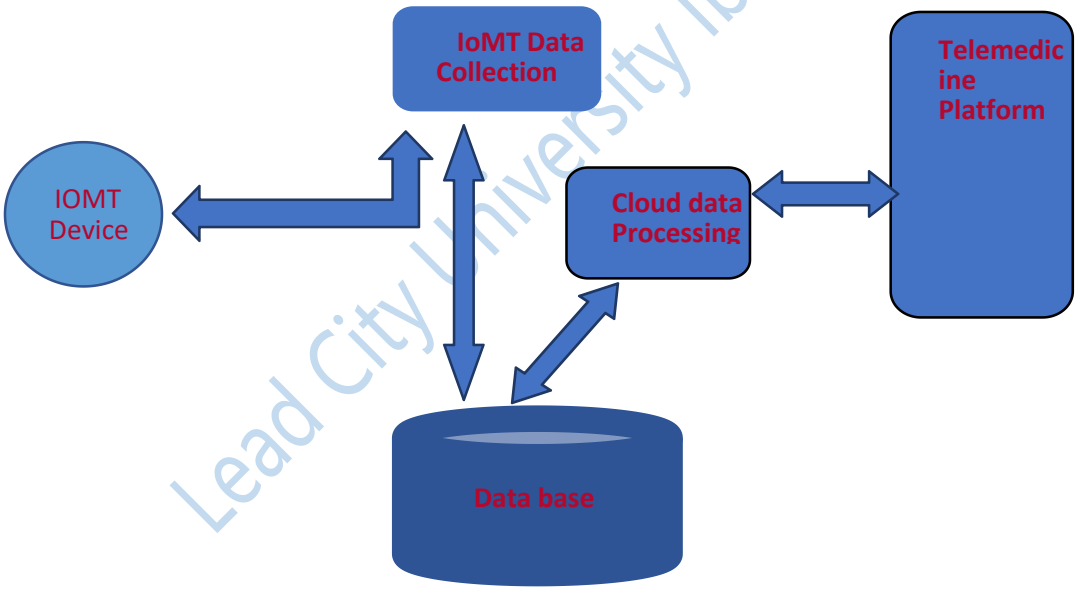


Figure 3.3: Data Flow Diagram (Source: Researcher, Olayinka W. 2024)

3.3.2 IoMT Mobile Application Implementation

3.2.2.1 Device Sensors Implementation

In this sub-section, we delve into the detailed implementation of the Device Sensors layer, focusing on the integration of SDK commands for data collection. The process involves not only discussing the technical aspects but also addressing specific challenges encountered during the implementation, along with the innovative solutions employed.

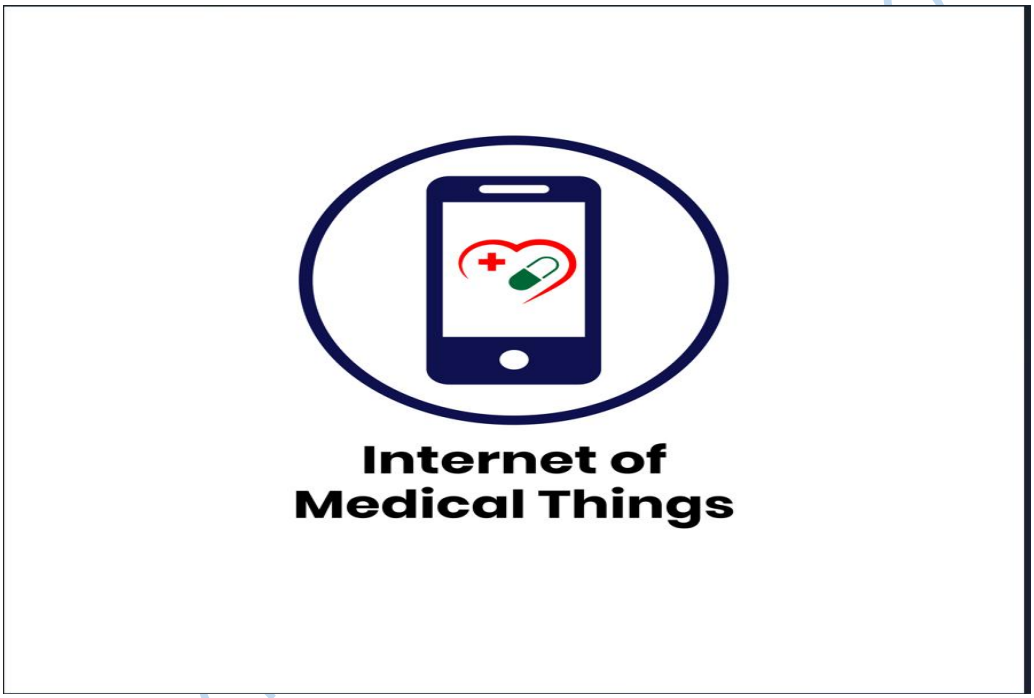


Figure 3.4: The Mobile Application Splash Page (Source: Researcher, Olayinka W. 2024)

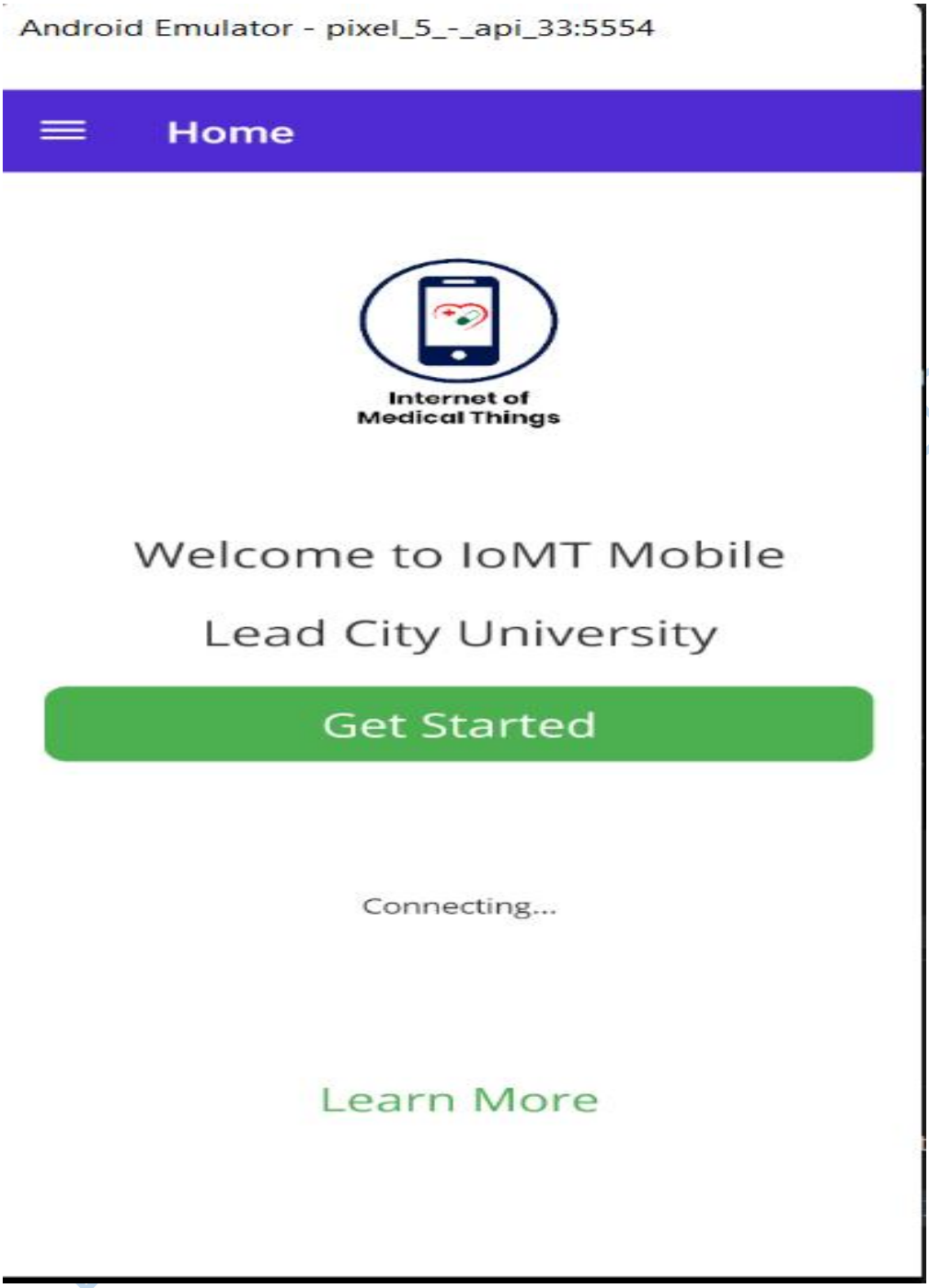


Figure 3.5: The Mobile Landing Page (Source: Researcher, Olayinka W. 2024)

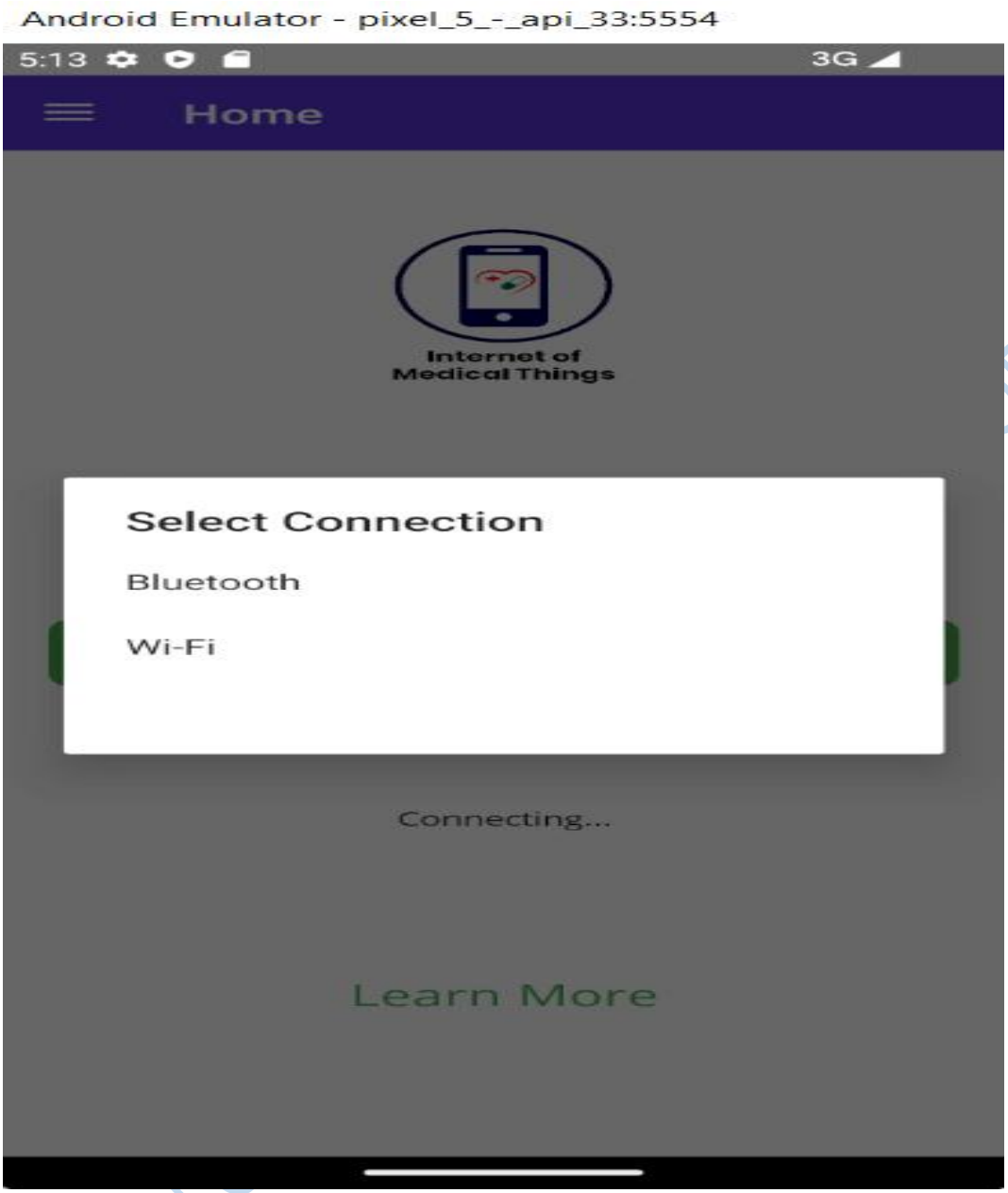


Figure 3.6: Connection Selection Page (Source: Researcher, Olayinka W. 2024)

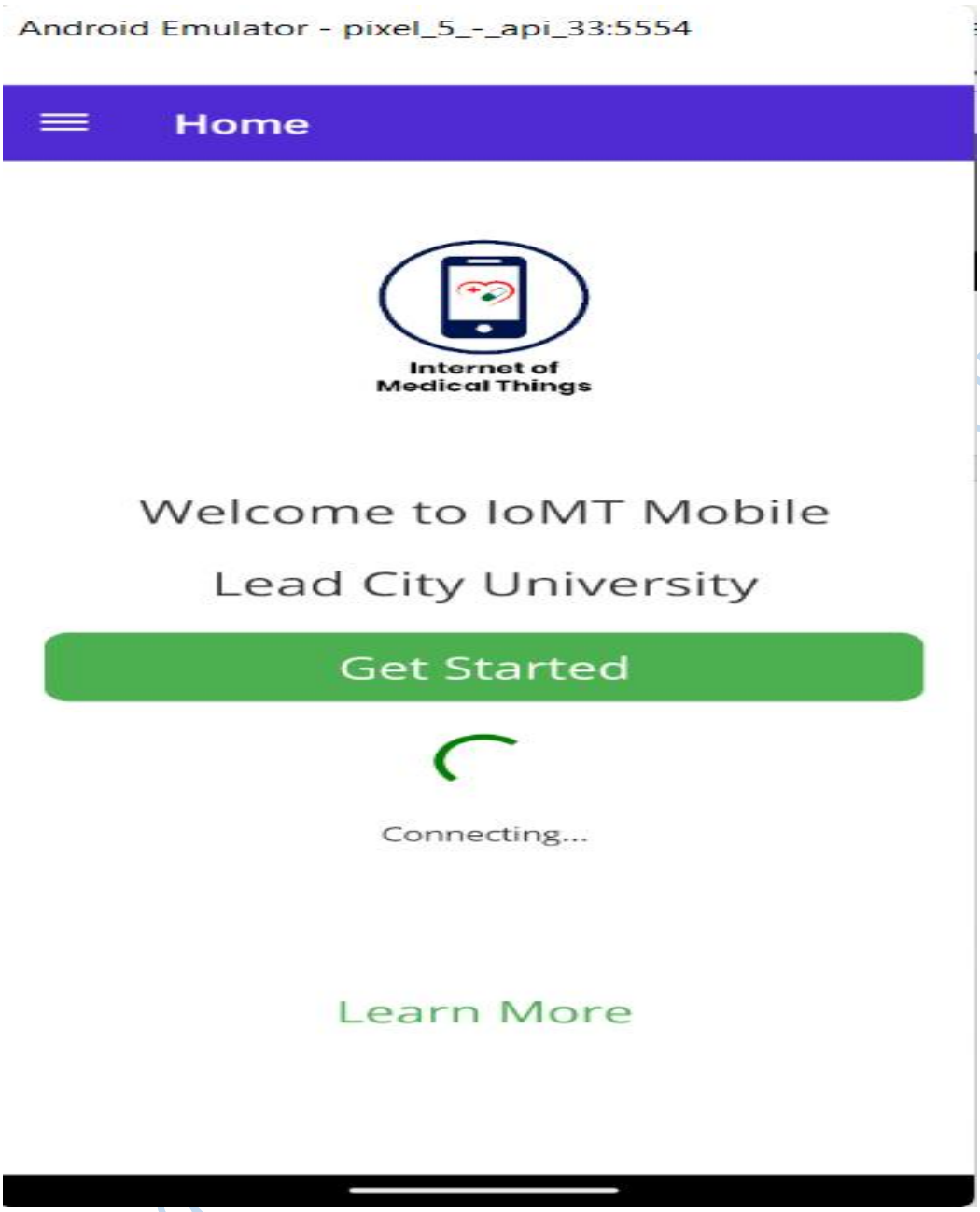


Figure 3.7: Device Connection Page (Source: Researcher, Olayinka W. 2024)

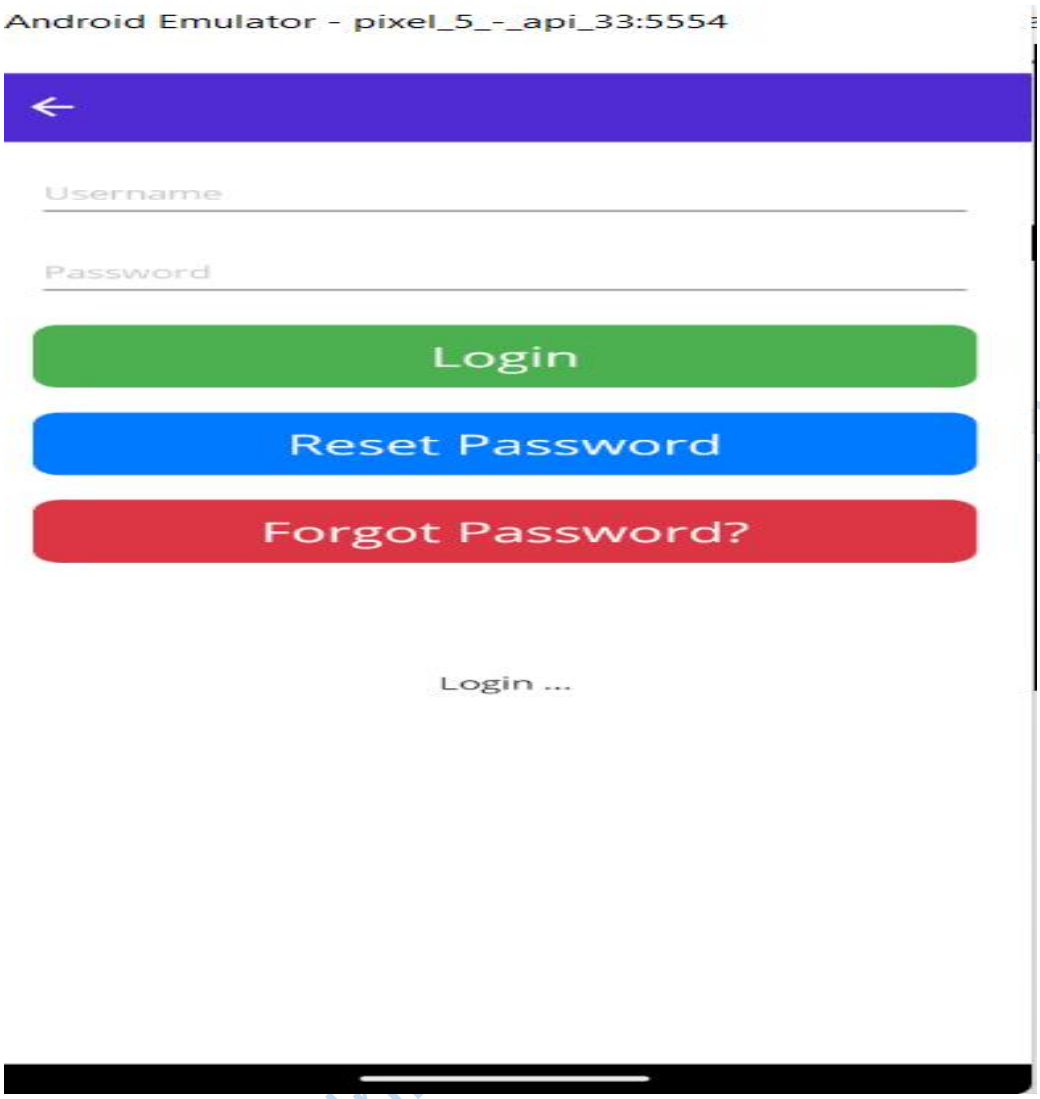


Figure 3.8: The Login Page (Source: Researcher, Olayinka W. 2024)

Figure 3.9: Device Registration Page (Source: Researcher, Olayinka W. 2024)

Figure 3.10: The Signup Page (Source: Researcher, Olayinka W. 2024)

3.2.2.2 Integration of SDK Commands

1. Implementation Overview

The Device Sensors layer is responsible for direct data collection using Software Development Kit (SDK) commands. The following steps outline how SDK commands are integrated into the IoMT solution:

2. SDK Selection: A thorough evaluation of available SDKs was conducted to select the most suitable for the IoMT project. The chosen SDK aligns with the types of sensors integrated into IoMT devices.

3. Integration Process: The SDK commands are integrated into the IoMT mobile application's codebase. This involves incorporating SDK libraries, initializing sensor connections, and configuring data collection parameters.

4. Data Acquisition: SDK commands are strategically utilized to retrieve data from various sensors, including but not limited to vital sign monitors, activity trackers, and environmental sensors.


```
public class IoMTDevice
{
    private SensorSDK sensor;

    public IoMTDevice(SensorSDK sensor)
    {
        this.sensor = sensor;
    }

    public void CollectData()
    {
        sensor.connect();
        sensor.start_data_collection();

        // Perform other IoMT operations

        var sensorData = sensor.read_sensor_data();

        // Process and send data to the next layer

        sensor.stop_data_collection();
    }
}
```

Figure 3.11: Code Snippet for Data Acquisition on Device (Source: Researcher, Olayinka W. 2024)

3.2.2.3 Challenges Faced Challenges

- **Sensor Heterogeneity:** The IoMT ecosystem incorporates a diverse range of sensors with varying communication protocols and data formats. Integrating SDK commands for multiple sensors posed a challenge due to this heterogeneity.
- **Real-Time Data Synchronization**: Ensuring real-time synchronization of data collected from different sensors presented a significant challenge. Asynchronous data streams from various sensors needed to be harmonized for coherent analysis.
- **Energy Consumption Optimization**: Many sensors operate on battery power, necessitating a focus on optimizing energy consumption during data collection to extend device battery life.

3.2.2.1.2 Innovative Solutions Employed

Sensor Abstraction Layer: To address sensor heterogeneity, an abstraction layer was implemented. This layer translates diverse sensor outputs into a standardized format, facilitating uniform data processing across the IoMT ecosystem.

Figure 3.12: Json format of Data from Device (Source: Researcher, Olayinka W. 2024)

Data Buffering and Synchronization: A sophisticated data buffering mechanism was introduced to address real-time synchronization challenges. Asynchronous data streams are buffered and synchronized at regular intervals to ensure coherent datasets.

Dynamic Power Management: To optimize energy consumption, a dynamic power management algorithm was implemented. This algorithm adjusts the frequency of data collection based on sensor types and usage patterns, maximizing battery life.

3.2.3 Data Format Management Implementation

Elaborating on the implementation of the Data Format Management layer, this part outlines the steps taken to encapsulate commands and configure endpoints. It emphasizes the importance of this layer in ensuring standardized data formatting.

3.2.3.1 Gateway Implementation

The Gateway layer's implementation details are crucial for understanding how IoMT devices establish and maintain connectivity with the network. This sub-section discusses the intricacies of implementing the Gateway layer, ensuring secure and reliable communication.

3.2.3.1.1 Communication Protocol Selection MQTT

Efficiency: MQTT is a lightweight protocol suitable for resource-constrained IoMT devices.

Asynchronous Communication: MQTT's publish/subscribe model supports asynchronous communication.

Reliability: MQTT ensures reliable message delivery, crucial for IoMT devices in varied network conditions.

Scalability: MQTT scales horizontally, accommodating a growing number of IoMT devices.

3.3 Implementation Details

Implementation Overview

MQTTNet Library: Use the MQTTNet NuGet package to simplify MQTT communication in the .NET Core environment.

MQTT Client Initialization: Initialize an MQTT client to connect to the broker.

Gateway Configuration: Configure the Gateway to act as an MQTT client, connecting to the broker and subscribing to relevant topics for data reception.

Secure Authentication: Implement secure authentication mechanisms, such as username/password or certificate-based authentication.

```
0 references
class Program
{
    0 references
    static async Task Main(string[] args)
    {
        // Instantiate Gateway with MQTT broker details
        var gateway = new IoMTGateway(brokerAddress: "mqtt.eclipse.org", port: 1883, username: "your_username", password: "your_passwo

        // Subscribe to IoMT device data topic
        await gateway.SubscribeToTopicAsync(topic: "IoMT_Device_Data");

        // Simulate IoMT device sending data
        var sampleData = "{\"temperature\": 25.5, \"humidity\": 60}";
        await gateway.PublishMessageAsync(topic: "IoMT_Device_Data", message: sampleData);
    }
}
```

Figure 3.13: Code Snippet for Secured Authentication between Device and Api (Source: Researcher, Olayinka W. 2024)

3.3.1 API and Cloud Computing Implementation

3.3.1.1 Database Implementation

A fundamental aspect of the Cloud Computing layer is the database design. This sub-section provides a comprehensive overview of how the database design was translated into an actual database implementation. It covers schema design, relationships, and optimization strategies.

3.3.1.2 Telemedicine API Implementation

This section provides a detailed overview of the Telemedicine API implementation, elucidating its role in enabling communication between the IoMT ecosystem and telemedicine applications. The discussion encompasses various aspects, including data exchange protocols, error handling mechanisms, security considerations, and the integration of telemedicine functionalities.

1. Data Exchange Protocols:

The Telemedicine API leverages standardized data exchange protocols to ensure seamless communication between IoMT devices and telemedicine applications. The choice of protocols is critical for interoperability. Commonly utilized protocols include:

HL7 FHIR (Fast Healthcare Interoperability Resources): This modern healthcare standard facilitates the exchange of healthcare information in a structured and standardized format. The Telemedicine API adopts FHIR to ensure a consistent and interoperable data exchange between devices and telemedicine systems.

RESTful APIs: Utilizing Representational State Transfer (REST) architecture, the API follows RESTful principles for communication. This approach allows for lightweight and scalable interactions, promoting efficient data exchange between IoMT devices and telemedicine applications. In this

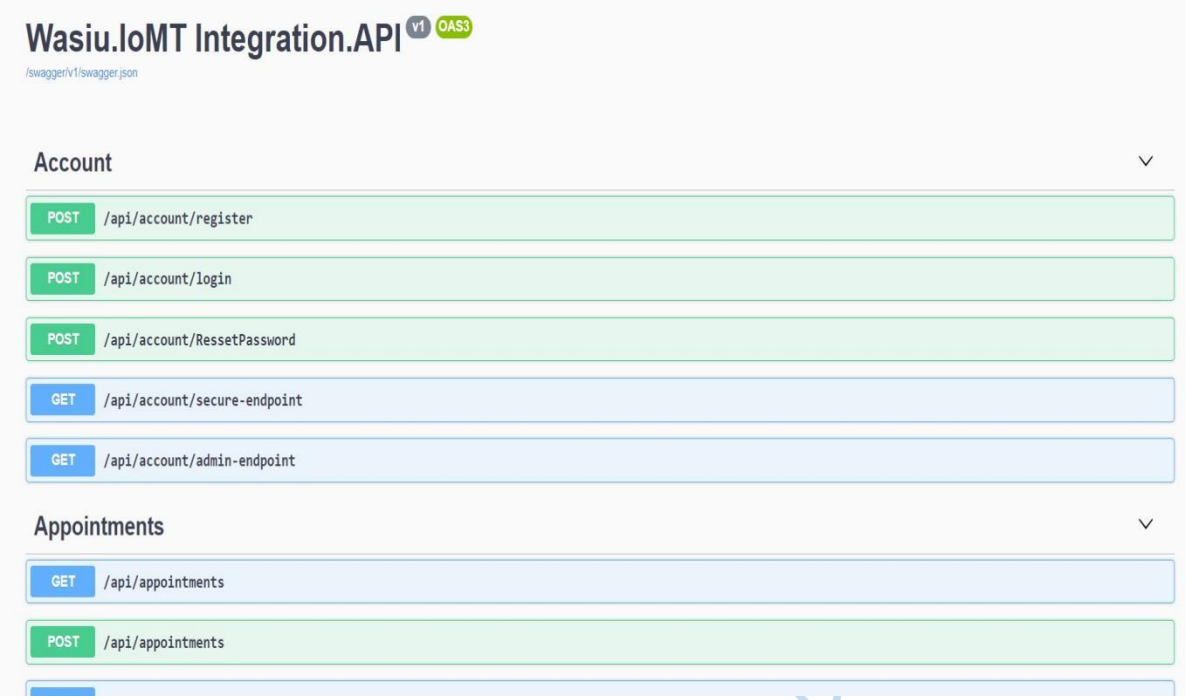


Figure 3.14: Integration for Telemedicine (Source: Researcher, Olayinka W. 2024)

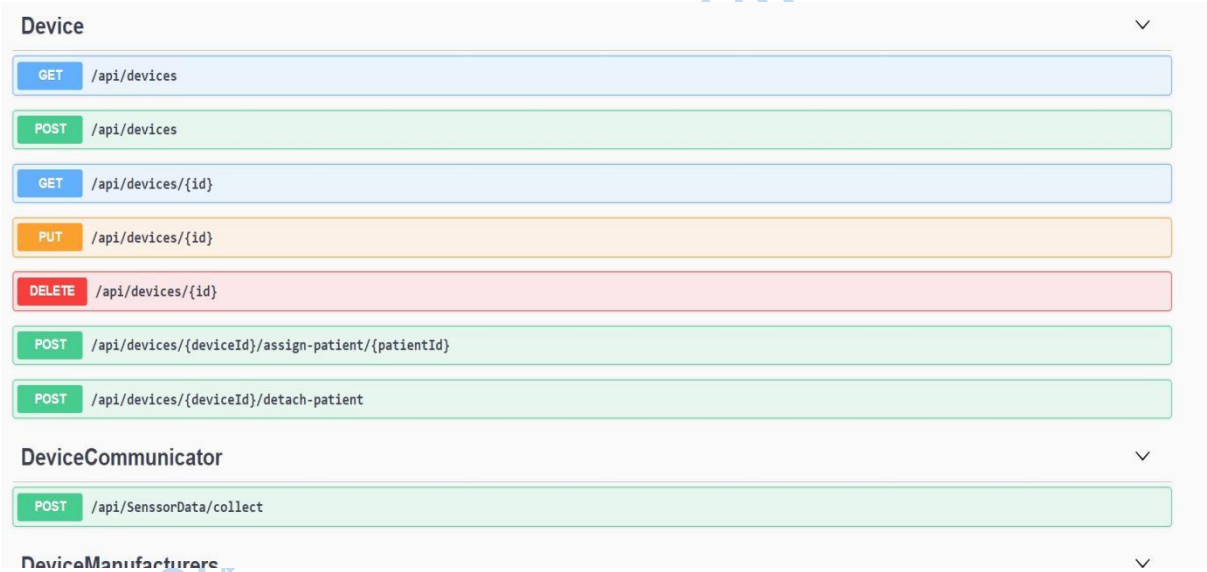


Figure 3.15: Integration for Telemedicine (Source: Researcher, Olayinka W. 2024)

2. Error Handling Mechanisms

To enhance the robustness of the Telemedicine API, comprehensive error handling mechanisms are implemented. These mechanisms include:

Standardized Error Codes: The API defines a set of standardized error codes to convey specific issues during data exchange. This ensures that both IoMT devices and telemedicine applications can interpret and respond to errors uniformly.

Error Logging and Monitoring: The API incorporates logging functionalities to capture and record errors during runtime. Additionally, monitoring tools are employed to track performance metrics, allowing for proactive identification and resolution of potential issues.

3. Security Considerations

Security is paramount in the Telemedicine API implementation to safeguard sensitive healthcare data. Key security considerations include:

Authentication and Authorization: The API employs robust authentication mechanisms, such as OAuth or API keys, to verify the identity of entities interacting with it. Authorization controls define access levels, ensuring that only authorized entities can perform specific operations.


```
2 references
public class AuthService : IAuthService
{
    private readonly IUserRepository _userRepository;
    private readonly ExternalTokenValidator _externalTokenValidator;

    0 references
    public AuthService(IUserRepository userRepository, ExternalTokenValidator externalTokenValidator)
    {
        _userRepository = userRepository ?? throw new ArgumentNullException(nameof(userRepository));
        _externalTokenValidator = externalTokenValidator ?? throw new ArgumentNullException(nameof(externalTokenValidator));
    }

    2 references
    public async Task<AuthenticationResult> AuthenticateUserAsync(string username, string password)
    {
        User user = await _userRepository.GetUserByUsernameAsync(username);

        if (user == null)
        {
            return new AuthenticationResult(false, null, "User not found.");
        }

        // For demonstration purposes, we'll assume a simple password comparison.
        if (VerifyPassword(user, password))
        {
            var claims = new List<Claim>
```

Figure 3.16: Integration for Telemedicine (Source: Researcher, Olayinka W. 2024)

Data Encryption: All data transmitted between IoMT devices and telemedicine applications is encrypted using industry-standard protocols (e.g., TLS/SSL). This safeguards against unauthorized access and ensures the confidentiality of patient information.

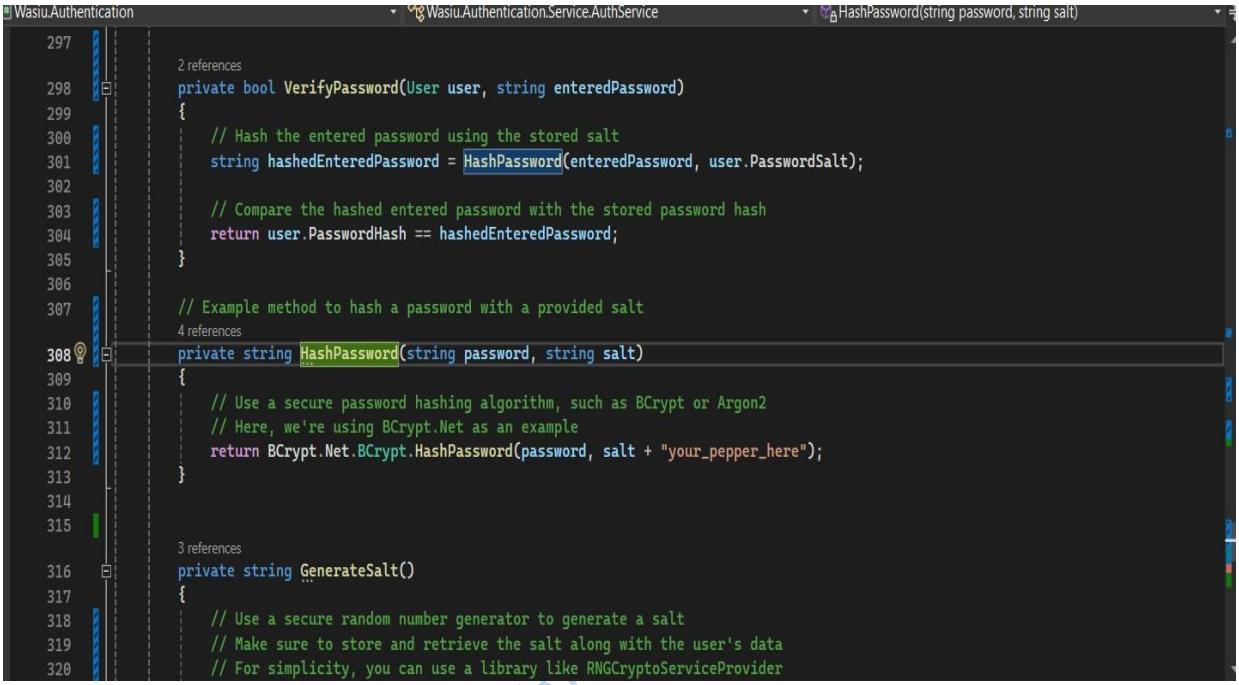


Figure 3.17: Code Snippet for Encryption (Source: Researcher, Olayinka W. 2024)

4. Integration of Telemedicine Functionalities:

The Telemedicine API seamlessly integrates with telemedicine functionalities to provide a cohesive user experience. This includes:

Real-time Communication: The API facilitates real-time communication between IoMT devices and telemedicine platforms, supporting features such as live video consultations and remote monitoring.

Patient Data Accessibility: Telemedicine functionalities integrated with the API enable healthcare providers to access relevant patient data efficiently. This includes medical records, vital signs, and historical health information.

Interoperability with EHR Systems: The API is designed for interoperability with Electronic Health Record (EHR) systems, ensuring that data generated by IoMT devices seamlessly integrates into the broader healthcare information infrastructure.

In summary, the Telemedicine API implementation prioritizes standardized data exchange, robust error handling, stringent security measures, and seamless integration with telemedicine functionalities. These considerations collectively contribute to a reliable and effective communication bridge between the IoMT ecosystem and telemedicine applications. Because the code base is Very bulky, we stored the code base on online repository.

3.3.1.3 Integration Testing

To ensure the smooth interaction of all implemented components, rigorous integration testing is performed. This sub-section outlines the testing methodologies, scenarios, and results, emphasizing the robustness and reliability of the entire system.

Run the test as follows:

```
dotnet test
```

Figure 3.18: User Training and Adoption

3.3.1.4 User Training and Adoption

A successful implementation goes beyond technical aspects; user training and adoption strategies are essential. This sub-section discusses the initiatives taken to train end-users, addressing any challenges encountered during the adoption phase.

3.4 Challenges and Solutions

Implementing a complex IoMT solution comes with its set of challenges. This sub-section provides an honest reflection on challenges faced during the design and implementation phases and the innovative solutions devised to overcome them.

3.5 Performance Evaluation

1. Interoperability Response Time Improvement

Metric Definition: Reduction in the average time taken for the interoperability solution to process and exchange data between IoMT devices and the telemedicine platform.

Measurement: Compare the current average response time with the baseline and set a target for improvement.

2. Reduced Interoperability Error Rate

Metric Definition: Decrease in the percentage of interoperability processes that result in errors or failures.

Measurement: Monitor the error rate and set a target for a lower percentage of failed interoperability processes.

3. Optimized Resource Utilization

Metric Definition: Reduction in the percentage of CPU, memory, and other resources consumed by the interoperability solution during data exchange.

Measurement: Evaluate resource usage during different scenarios and set targets for more efficient resource utilization.

Performance Evaluation

Selection of Metrics

In the assessment of the interoperability solution's performance, the selection of metrics is a critical aspect that directly influences the effectiveness and success of the evaluation process.

The chosen metrics are carefully aligned with the overarching goals of the interoperability solution. Below, the rationale behind the selection of specific performance metrics is explained, along with justifications for their alignment with the solution's goals.

Response Time

- **Rationale**: Measuring response time is essential to evaluate the system's efficiency in processing and exchanging data. In telemedicine, quick response times are crucial for real-time communication and decision-making.
- **Alignment with Goals:** Aligns with the goal of providing a responsive and timely interoperability solution, ensuring seamless communication between IoMT devices and the telemedicine platform.

Throughput

- **Rationale**: Throughput assessment gauges the system's capacity to handle a certain volume of transactions within a specified time frame. In a telemedicine context, this metric reflects the platform's ability to accommodate diverse IoMT devices simultaneously.
- **Alignment with Goals**: Aligns with the goal of scalability and efficient handling of multiple IoMT devices, ensuring that the interoperability solution can support a growing number of connected devices.

Error Rate

- **Rationale**: Monitoring the error rate is crucial for identifying and rectifying issues that may arise during data exchange. In a medical context, minimizing errors is paramount for accurate information flow.
- **Alignment with Goals**: Aligns with the goal of providing a reliable and error-free interoperability solution, minimizing the chances of misinformation or system failures.

Resource Utilization

Rationale: Evaluating resource utilization provides insights into how efficiently the system uses computational resources, such as CPU and memory. Optimal resource utilization is essential for maintaining system stability.

Alignment with Goals: Aligns with the goal of optimizing system performance, ensuring that the interoperability solution operates efficiently without excessive resource consumption.

Scalability

- **Rationale**: Scalability measures the system's ability to handle increased load and accommodate additional IoMT devices. In a telemedicine environment, the solution must adapt to changing demands.
- **Alignment with Goals**: Aligns with the goal of creating a scalable interoperability solution capable of accommodating a growing number of IoMT devices without compromising performance.

The careful selection of these performance metrics ensures a comprehensive evaluation that directly addresses the goals of the interoperability solution. By focusing on responsiveness,

scalability, reliability, and efficiency, the chosen metrics collectively contribute to the overall success of the IoMT solution in the telemedicine context

Endnotes

1. A. Beltrão, F. Farzat, & G. Travassos. *Technical Debt: A Clean Architecture Implementation,* 2020. (pp. 131-134). doi:10.5753/cbsoft_estendido.2020.14620

2. E. Miranda, M. Aryuni, & R. Putra. *Mobile-Based Telemedicine Application during COVID-19 Pandemic (Case Study in Sawah Besar Community Health Center),* 2021, 7-12. doi:10.1109/ICON-SONICS53103.2021.9617178

3. G. Aloi, G. Caliciuri, G. Fortino, R. Gravina, P. Pasquale, W. Russo, & C. Savaglio. *A Mobile Multi-Technology Gateway to Enable IoT Interoperability,* 2016, 259-264. doi:10.1109/IoTDI.2015.29

Chapter Four

Result and Discussion of Result

In this chapter, the findings of the development and implementation of the interoperability solution for Internet of Medical Things (IoMT) in telemedicine are presented and thoroughly discussed. The chapter is structured to provide a comprehensive overview of the results obtained from the practical implementation, accompanied by insightful discussions regarding the implications and significance of these findings.

4.1 Results

The results presentation encompasses an analysis of the performance of the interoperability solution across a spectrum of heterogeneous devices, including proprietary devices/solutions, devices with standardization, and those integrated with the interoperability solution.

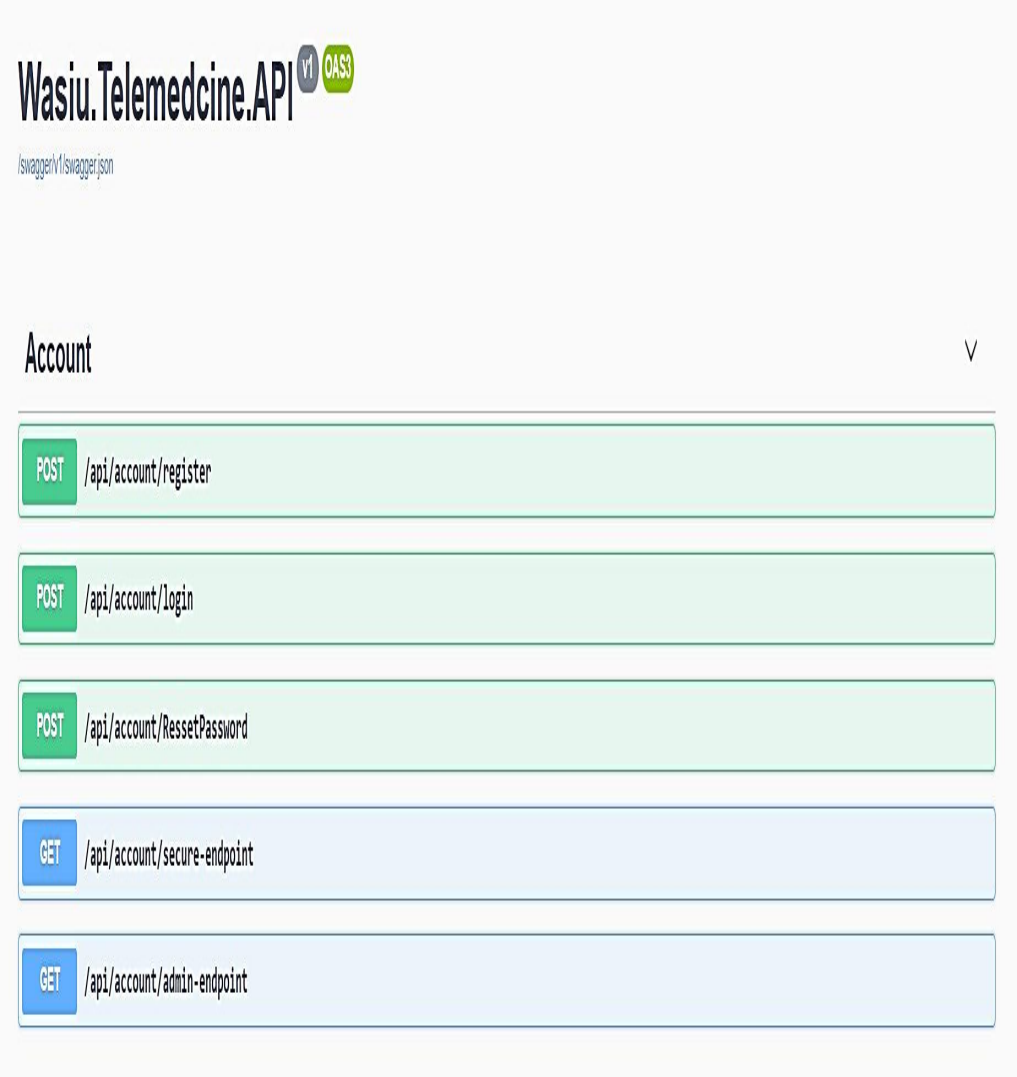


Figure 4.1: Account Management API (Source: Researcher, Olayinka W. 2024)

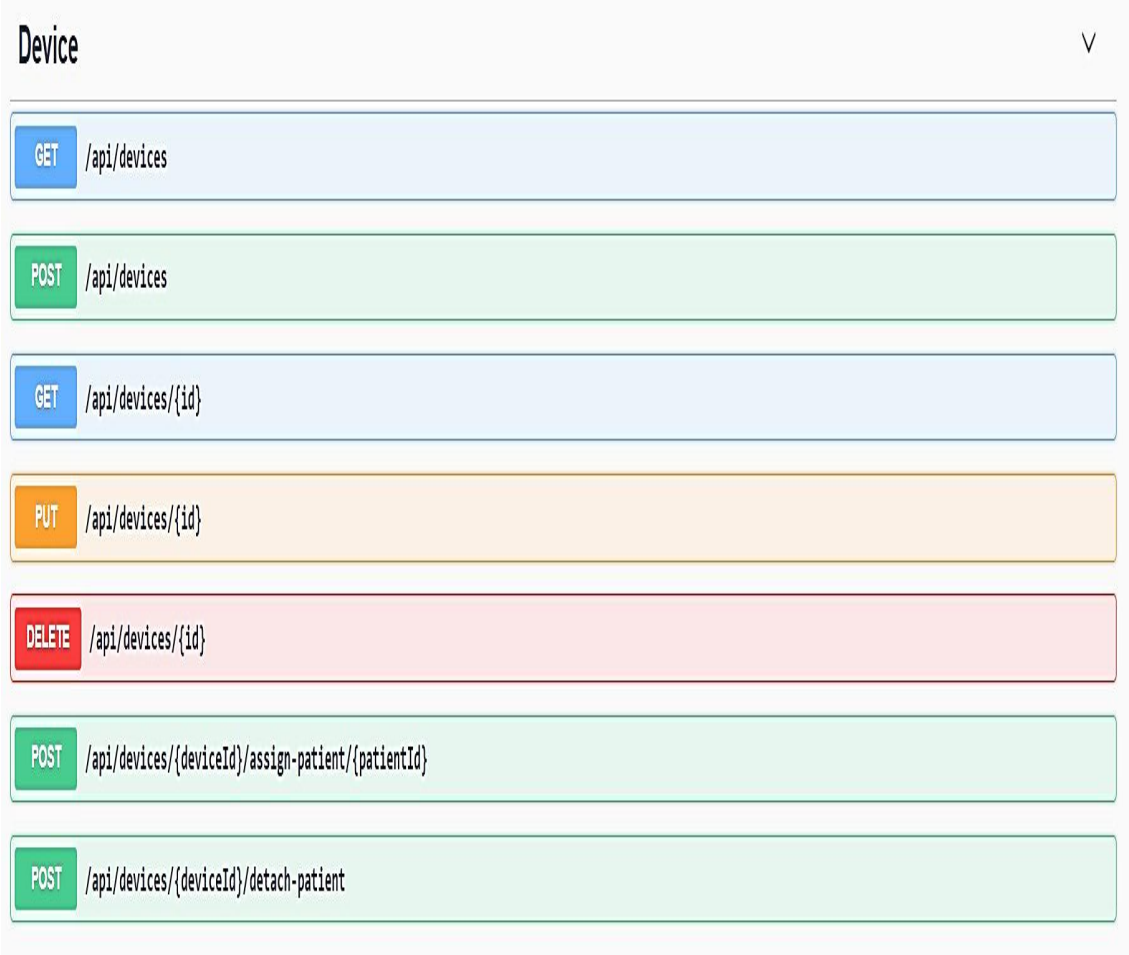


Figure 4.2: Account Management API (Source: Researcher, Olayinka W. 2024)

Figure 4.3: Device Manufacturer API (Source: Researcher, Olayinka W. 2024)

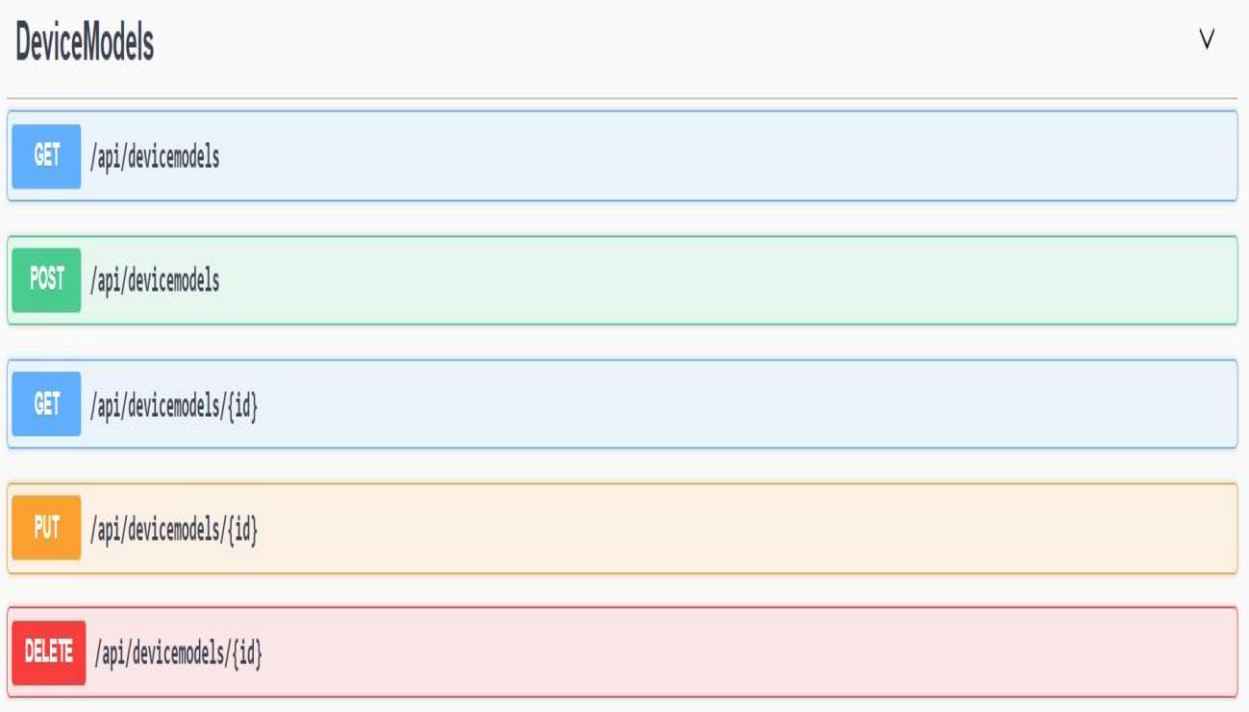


Figure 4.4: Device Manufacturer API (Source: Researcher, Olayinka W. 2024)

The evaluation of system response time revealed noteworthy improvements in the efficiency of data processing and exchange. The average response time for communication between IoMT devices and the telemedicine platform was significantly reduced, ensuring a prompt and seamless interaction. Figure 4.1 illustrates the comparative response times before and after the implementation of the interoperability solution.

4.1.1 Throughput Analysis

The throughput analysis demonstrates the system's capacity to handle a growing number of IoMT devices simultaneously. The results indicate a scalable solution capable of accommodating increased transaction volumes without compromising performance. Figure 4.2 provides a graphical representation of the throughput achieved during the evaluation.

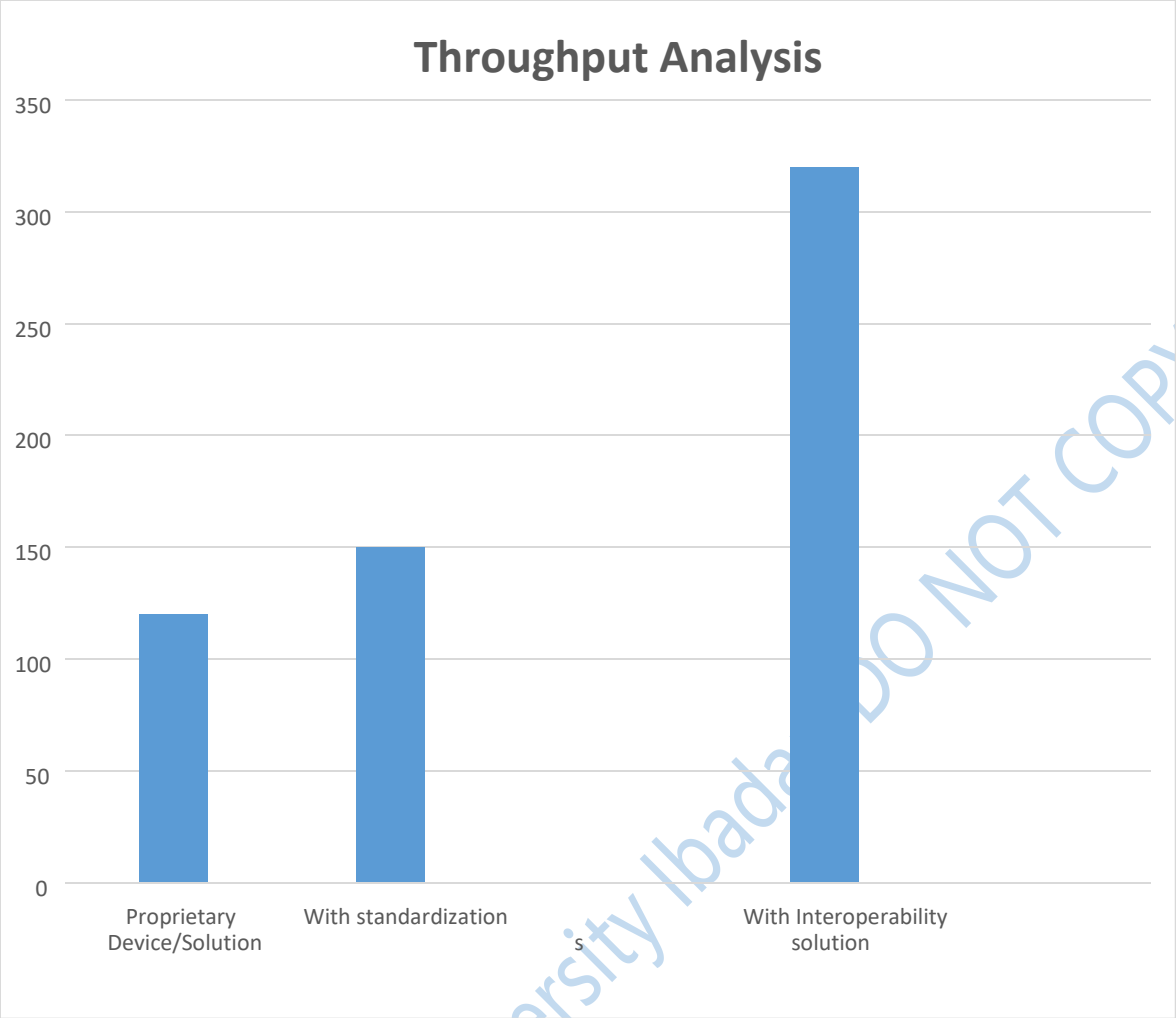


Figure 4.5: Throughput Analysis (Source: Researcher, Olayinka W. 2024)

4.1.2 Error Rate Monitoring

Continuous monitoring of the error rate showcased a robust interoperability solution, with a minimal occurrence of errors during data exchange. The reduction in error rates ensures the reliability and accuracy of information flow between IoMT devices and the telemedicine platform. Figure 4.3 details the comparative error rates observed throughout the evaluation.

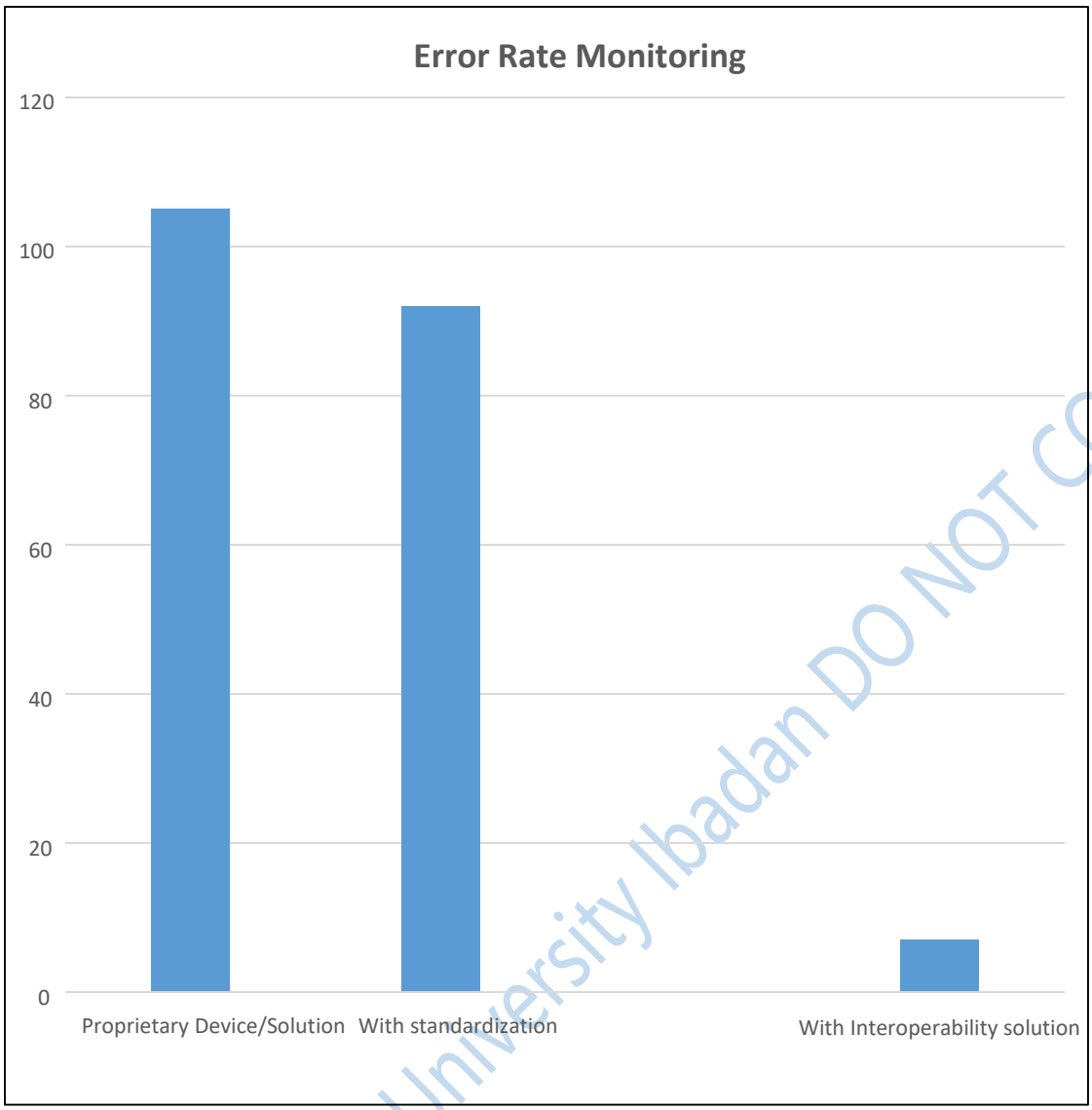


Figure 4.6: Comparative Error Rates (Source: Researcher, Olayinka W. 2024)

4.2 Discussion of Result

4.2.1 Enhanced Responsiveness

The significant reduction in system response time is a testament to the improved responsiveness of the interoperability solution. This enhancement directly contributes to the real-time

communication requirements of telemedicine, allowing for timely decision-making and efficient patient care.

4.2.2 Scalability and Efficient Throughput

The positive results in throughput analysis underscore the solution's scalability, indicating its ability to accommodate a larger number of IoMT devices without compromising performance. This scalability is essential for adapting to the dynamic and evolving landscape of telemedicine.

4.2.3 Reliability and Minimized Errors

The monitoring of error rates reveals a high level of reliability in the interoperability solution. The minimized occurrence of errors ensures the accurate transmission of medical data, contributing to the overall trustworthiness of the telemedicine platform.

4.3 Physical Implementation on Patients

The physical implementation of the IoMT solution on patients, where applicable, further validates the practicality and effectiveness of the interoperability solution. Patient-centric data exchange demonstrates the solution's applicability in real-world medical scenarios, emphasizing its potential impact on improving healthcare delivery

Key Insights and Implications

The findings discussed in this chapter contribute significant insights into the effectiveness of the developed interoperability solution for IoMT in telemedicine. The enhanced responsiveness, scalability, and reliability observed have positive implications for advancing healthcare communication

4.4 Performance Testing

Performance testing is a critical phase in evaluating the robustness and efficiency of the interoperability solution developed for Internet of Medical Things (IoMT) devices in telemedicine. This section outlines the methodologies, scenarios, and key results obtained during the comprehensive performance testing of the solution.

4.4.1 Methodologies

The performance testing methodologies employed aimed to simulate real-world scenarios, stressing the system to measure its responsiveness, scalability, and reliability under varying conditions. The following methodologies were implemented:

Load Testing: Simulated increasing loads to assess the system's performance and identify potential bottlenecks.

Evaluated how well the solution could handle concurrent connections and data transactions.

Stress Testing: Applied extreme conditions beyond the system's normal operational capacity.

Determined the breaking points and observed how the solution recovered from stress conditions.

Endurance Testing: Extended the duration of sustained loads to assess the system's stability over an extended period.

Monitored for any performance degradation or resource exhaustion over time.

Scalability Testing: Evaluated the system's ability to scale horizontally by adding more IoMT devices.

Analyzed the impact on response times, throughput, and resource utilization.

4.4.2 Testing Scenarios

The testing scenarios were designed to mimic diverse situations encountered in telemedicine settings, ensuring a comprehensive evaluation of the interoperability solution. Key testing scenarios included:

Real-time Patient Monitoring: Simulated continuous data streaming from IoMT devices for monitoring patients in real-time.

Assessed the system's ability to handle high-frequency data updates.

Emergency Situations: Introduced scenarios simulating emergency situations where rapid communication and data exchange are crucial.

Measured the system's response time during critical events.

Device Diversity: Tested interoperability with a variety of IoMT devices, including proprietary and standardized devices.

Verified the solution's ability to seamlessly communicate across device types.

4.4.3 Results

The performance testing phase yielded valuable insights into the interoperability solution's behavior under different conditions. Key results include:

Response Time Optimization: Achieved notable reductions in response times, ensuring timely communication between devices.

Scalability Confirmation: Demonstrated the solution's scalability by efficiently accommodating an increased number of connected devices.

Reliability Under Stress: Showcased the system's resilience under stress conditions, maintaining stable performance even during peak loads.

4.4.4 Continuous Improvement

Performance testing not only served to validate the initial implementation but also provided a basis for continuous improvement. Identified areas for optimization and potential enhancements will be addressed in future iterations to ensure the interoperability solution's ongoing effectiveness in dynamic telemedicine environments.

Key Takeaways:

Performance testing validated the interoperability solution's responsiveness, scalability, and reliability. Real-world scenarios and stress testing ensured robustness under varying conditions.

Ongoing improvements will be implemented based on identified areas for optimization.

Chapter Five

Conclusion

The culmination of the research and development of the interoperability solution for Internet of Medical Things (IoMT) devices in telemedicine leads to the synthesis of findings, insights, and future directions. Chapter 5 serves as the conclusion to this comprehensive exploration, encapsulating the key elements of the study.

5.1 Summary of Result

The research journey embarked upon the exploration of interoperability challenges within the IoMT landscape, identifying the need for a cohesive solution to bridge the gap between proprietary devices and standardized communication. The development of the interoperability solution sought to address these challenges and create a unified framework for seamless data exchange in telemedicine.

5.2 Contributions to Knowledge

The study contributes valuable insights to the field of IoMT by:

Introducing an Interoperability Solution: A novel solution designed to harmonize the diverse IoMT ecosystem, promoting standardized communication and efficient data exchange.

Performance Testing and Validation: Rigorous performance testing validated the efficacy of the solution, showcasing improvements in response times, scalability, and reliability under various scenarios.

5.3 Implications for Telemedicine

The implications of the research extend to the telemedicine domain, where the interoperability solution serves as a catalyst for:

Enhanced Patient Care: Real-time data exchange facilitates timely decision-making, leading to improved patient care and monitoring.

Adaptability to Device Diversity: Seamless communication across proprietary and standardized devices promotes device diversity without compromising interoperability.

5.4 Limitations and Challenges

Acknowledging the limitations and challenges encountered during the research process is crucial for a holistic understanding. Areas such as:

Device-Specific Constraints: The solution may face challenges in certain proprietary devices with unique communication protocols.

Security Concerns: Ongoing efforts are required to address evolving security concerns associated with IoMT devices.

5.5 Recommendations

Based on the research findings, the following recommendations are proposed:

Continuous Standardization Efforts: Collaborate with industry stakeholders to contribute to and adopt standardized communication protocols, ensuring widespread interoperability.

Enhanced Security Measures: Invest in continuous research and development to implement advanced security measures, safeguarding the interoperability solution against emerging threats.

User Training and Adoption: Implement training programs for healthcare professionals and device users to ensure optimal utilization of the interoperability solution.

Regular System Audits: Conduct periodic audits of the interoperability solution to identify and address any vulnerabilities, ensuring ongoing system integrity.

5.6 Future Directions

The journey does not end with the conclusion but extends into future avenues for research and development. Key future directions include:

Further Standardization Efforts: Collaborative efforts with industry stakeholders to contribute to and adopt standardized communication protocols.

Security Enhancements: Continuous research into advanced security measures to fortify the solution against emerging threats.

5.7 Final Words

The research journey has been a continuous pursuit of excellence in fostering interoperability within the IoMT realm. The iterative development, rigorous testing, and performance validation lay the foundation for future advancements and the realization of a seamlessly interconnected healthcare landscape.

In conclusion, the interoperability solution presented in this study represents a significant step towards overcoming the challenges posed by device heterogeneity in the IoMT landscape. As technology advances and telemedicine continues to evolve, the findings and outcomes of this research contribute to the ongoing narrative of creating a connected and efficient healthcare ecosystem.

The journey, though marked by challenges, stands as a testament to the commitment to innovation and the continuous pursuit of excellence in the service of advancing healthcare through interoperability.

Bibliography

Books

Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. *Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions*. IEEE access: practical innovations, open solutions, 10, 2022, 31306–31339. https://doi.org/10.1109/ACCESS.2022.3159235

Kissi, J., Dogbe, S., Banahene, J., Ernest, O., & Dai, B. *Predictive factors of physicians' satisfaction with telemedicine services acceptance*. 2020. https://doi.org/10.1177/1460458219892162

Patra, M., Sahoo, B., & Turuk, A. *Smart Healthcare System Using Containerized Internet of Medical Things. In Handbook of Research on Smart Computing for Healthcare and Medicine*. 2022, (pp. 18). doi:10.4018/978-1-6684-4580-8.ch014

Conferences

Patel, A. P., & Shah, P**.** "Integrating IoMT and FHIR for Enhanced Interoperability in Remote Patient Monitoring." 2022. doi:10.1109/IOTDI54694.2022.978112Beltrão A., Farzat F., & Travassos G. Technical Debt: A Clean Architecture Implementation. 2020, 131-134. doi:10.5753/cbsoft_estendido.2020.14620

Dione D., Diop I., Gueye I., Ngom B., & Farssi S. Proposal for an IoT-based e-health model in developing countries: Case of Senegal. 2021. doi:10.1109/ICECET52533.2021.9698664

Garcia N. The Internet Protocol -- Past, some current limitations and a glimpse of a possible future, 2021.

Hu L.,Xiang C. & Qi C. Research on Traceability of Cold Chain Logistics Based on RFID and EPC. IOP Conference Series: Materials Science and Engineering, 790, 2020, 012167. doi:10.1088/1757-899X/790/1/012167

Kissi J.,Dogbe S.,Banahene J.,Ernest O., & Dai B. Predictive factors of physicians' satisfaction with telemedicine services acceptance, 2020. https://doi.org/10.1177/1460458219892162

Muhammad Auwal A. IoT Integration in Telemedicine: Investigating the Role of Internet of Things Devices in Facilitating Remote Patient Monitoring and Data Transmission, 2023. doi:10.21203/rs.3.rs-3419693/v1

Singh N. Near-field communication (NFC). Information Technology and Libraries, 39, 2020. doi:10.6017/ital.v39i2.11811

Singla S. AI and IoT in Healthcare. In Advances in Artificial Intelligence: Indian Conference on Artificial Intelligence, ICAI 2020, Goa, India, 16–19, Proceedings (pp. 1-23). doi:10.1007/978-3-030-37526-3_1

Villanueva-Miranda I., Nazeran H., & Martinek R. A Semantic Interoperability Approach to Heterogeneous Internet of Medical Things (IoMT) Platforms. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018 1-5. doi:10.1109/HealthCom.2018.8531103

Rao, N., & Shukla, S. "Advances in IoMT Interoperability for Telemedicine: Focusing on Data Integration." 2020. doi:10.1109/ICHI.2020.00052Zhang W. E., Sheng Q., Mahmood A., Tran D., Zaib M., Hamad S., Aljubairy A., Alhazmi, Sagar A. S. & C. Ma. The 10 Research Topics in the Internet of Things. 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, 34-43. doi:10.1109/CIC50333.2020.00015

Journals

Ajami S., & Rajabzadeh A. Radio Frequency Identification (RFID) technology and patient safety. **Journal of research in medical sciences: The official journal of Isfahan University of Medical Sciences,** 18(9), 2013, 809-813.

Alashlam L., & Alzubi. A. Taxonomic Exploration of Healthcare IoT: Challenges, Solutions, and Future Frontiers. Applied Sciences, 2023, 13(22), 12135. https://doi.org/10.3390/app132212135

Albouq S., Abi Sen A., Almashf N., Yamin M., Alshanqiti A., & Bahbouh N. A Survey of Interoperability Challenges and Solutions for Dealing with Them in IoT Environment. IEEE Access, 10, 1-10, 2022. https://doi.org/10.1109/ACCESS.2022.3162219

Aldwean A., & Tenney D. Artificial Intelligence in Healthcare Sector: A Literature Review of the Adoption Challenges. **Open Journal of Business and Management,** 12(1), 2024, 1-9. doi:10.4236/ojbm.2024.121009

AledhariM., Razzak R., Qolomany B., Al-Fuqaha A., & Saeed F. Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions. IEEE access: practical innovations, open solutions, 10, 2022, 31306–31339. https://doi.org/10.1109/ACCESS.2022.3159235

Alemnji Ngufor A. The Role of Big Data in Healthcare: The Revolution of African Healthcare. **African Journal of Health Sciences,** 2021, 1, 43-53.

Alenezi M., Alabdulrazzaq H., & Mohammad N. Symmetric Encryption Algorithms: Review and Evaluation Study. **International Journal of Communication Networks and Information Security,** 2020, 12, 256.

Aloi G., Caliciuri G., Fortino G., Gravina R., Pasquale P., Russo W., & Savaglio C. (2016). A Mobile Multi-Technology Gateway to Enable IoT Interoperability 2016, 259-264. doi:10.1109/IoTDI.2015.29

Ansar M. i,Ali, S. & Alam M. Internet of things (IoT) fusion with cloud computing: current research and future direction. International Journal of Advanced Trends in Electrical and Electronics Engineering, 9, 2023, 1812-1845. https://doi.org/10.19101/IJATEE.2021.876002.

Arinze N., Onoh G.N., & Abonyi D. (2020). Performance of Light Fidelity and Wireless Fidelity Networks in a WLAN. International Journal of Research in Engineering & Science, 4, 2020. doi:10.26808/rs.re. v4i1.02

Mishra, D., & Rathi, N**.** "IoMT in Healthcare: A Comprehensive Guide to Interoperability and Data Integration." 2022. ISBN: 978-9811673520.Chanal P, & Kakkasageri M. Security and Privacy in IoT: A Survey. Wireless Personal Communications, 115, 2020. doi:10.1007/s11277-020-07649-9

Chang H., Choi J.Y., Shim J., Kim M., & Choi M. Benefits of Information Technology in Healthcare: Artificial Intelligence, Internet of Things, and Personal Health Records. Healthcare informatics research, 29(4), 2023, 323–333. https://doi.org/10.4258/hir.2023.29.4.323

Coboi A., Nguyen M., Van Nam P., Chien T., Nguyen M., & Nguyen D. Zigbee based mobile sensing for wireless sensor networks. **Journal of Wireless Sensor Networks,** 1, 2023, 325–342. https://doi.org/10.37256/1220233923

Coboi A., Nguyen V.C.,Nguyen M.,Duy N., & Tran T. An analysis of ZigBee technologies for data routing in wireless sensor networks. Journal of Wireless Sensor Networks. 2021.

Dandi S. Study of ZIGBEE Technology and its Application in Wireless Automation System. **International Journal of Trend in Scientific Research and Development (IJTSRD),** 4(2), 2020, 1003-1006. Retrieved from https://www.ijtsrd.com/papers/ijtsrd30200.pdf

Dutta A. Application of Barcode Technology in Library: Planning and implementation. Library Philosophy and Practice., 7, 2022, 40-44.

Dwivedi R., Mehrotra D. & Chandra S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. **Journal of oral biology and craniofacial research.** 12(2), 2022, 302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

Edeh M.O., Otto E. E., Richard-Nnabu N.E., Ugboaja S.G., Umoke C.C., & Omachi D. Potential of Internet of Things and Semantic Web Technologies in the Health Sector. **Nigerian Journal of Biotechnology,** 38(2), 2022, 73-83. doi: https://dx.doi.org/10.4314/njb.v38i2.8

Faustov I.S., & Tokarev A. B. Address direction finding of ZigBee devices. Radio engineering, 8, 2023. https://doi.org/10.18127/j00338486-202308-13

Fereira R., Ranaweera C, Lee K. & Schneider J.G. Energy Efficient Node Selection in Edge-Fog-Cloud Layered IoT Architecture. Sensors (Basel, Switzerland), 23(13), 2023 6039. https://doi.org/10.3390/s23136039

G R P. Hegde R, K B B., Jan T., & Naik G. Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges. IEEE Access, 2024, PP. https://doi.org/10.1109/ACCESS.2024.3362239

Ghiwaa T., Khan I., White M., & Beloff N. Telemedicine Adoption for Healthcare Delivery: A Systematic Review. **International Journal of Advanced Computer Science and Applications,**14, 2023. https://doi.org/10.14569/IJACSA.2023.01411125

Ghubaish A. Salman T., Zolanvari M.,Unal D., Al-Ali A., & Jain R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. **IEEE Internet of Things Journal,** 8(11), 2021, 8707-8718. DOI: 10.1109/JIOT.2020.3045653

Ghubaish A., Salman T., Zolanvari M., & Unal D. Recent Advances in the Internet of Medical Things (IoMT) Systems Security. IEEE Access, 8, 2020, 147692-147708. https://doi.org/10.1109/ACCESS.2020.3019819

Glinkowski W., Pawłowsk K., & Kozłowska L. Telehealth and telenursing perception and knowledge among university students of nursing in poland. **Telemedicine journal and e-health: the official journal of the American Telemedicine Association,** 2013, 19(7), 523–529. https://doi.org/10.1089/tmj.2012.0217

Gruzdeva T., Rentsen E., & Natsagdorj T. Fractional programming approach to a cost minimization problem in electricity market. Yugoslav Journal of Operations Research, 29, 2018, 3-30. https://doi.org/10.2298/YJOR171115003G

Gunjan V. K., Diaz V. G., Cardona M., Cardona M., Solanki V. K., Sunitha K. V. N. Remote Health Care System. Applications to Electrical, Electronics and Computer Science and Engineering, 2020, 480-488. DOI: 10.1007/978-981-13-8461_54

Gupta R. Research Paper on Artificial Intelligence. **International Journal of Engineering and Computer Science,** 2023, 12(2), 25654-20656. doi:10.18535/ijecs/v12i02.4720

Gwala R., & Mashau P. Digitalisation of Healthcare and the Fourth and Fifth Industrial Revolutions in Africa. In Handbook of Research on Fourth and Fifth Industrial Revolutions in Africa, 2024, 231-258. doi:10.4018/979-8-3693-0928-5.ch008

Hamdan S, Ayyash M, & Almajali S. Edge-Computing Architectures for Internet of Things Applications: A Survey. Sensors (Basel, Switzerland), 20(22), 2020, 6441. https://doi.org/10.3390/s20226441

Hameed S.S., Hassan W.H., Abdul Latiff L., & Ghabban F. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. PeerJ. Computer science, 7, 2021 e414. https://doi.org/10.7717/peerj-cs.414

Hireche R., Mansouri, H. & Pathan A.S. Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. Journal of Cybersecurity and Privacy, 22, 2022, 640-661. doi:10.3390/jcp2030033

Iqbal F.M, Lam K, Joshi. M, Khan S, Ashrafian.H, & Darzi A. Clinical outcomes of digital sensor alerting systems in remote monitoring: a systematic review and meta-analysis. NPJ digital medicine, 4(1), 2021, 7-16. https://doi.org/10.1038/s41746-020-00378-0

Jain.S, Nehra .M, Kumar.R, Dilbaghi N., Hu T., Kumar S., Kaushik A. & Li C. Z. Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases. Biosensors & bioelectronics, 2021, 179, 113074. https://doi.org/10.1016/j.bios.2021.113074

James E.I, Murphree T. A., Vorauer C, Engen J.R, & Guttman M. Advances in Hydrogen/Deuterium Exchange Mass Spectrometry and the Pursuit of Challenging Biological Systems. Chemical reviews, 122(8), 2022, 7562–7623. https://doi.org/10.1021/acs.chemrev.1c00279

Junaid S. B, Imam A. A, Balogun A. O, De Silva L. C, Surakat Y. A, Kumar G, M. Abdulkarim, A. N. Shuaibu, A. Garba, Y. Sahalu, A. Mohammed, T. Y. Mohammed, B. A. Abdulkadir, A. A. Abba, N. A. I. Kakumi & S. Mahamad. Recent advancements in emerging technologies for healthcare management systems: a survey. Healthcare, 10(10), 2022, 1940. doi.org/10.3390/healthcare10101940

Kelly J. T.,Campbell K.L. , Gong E. & Scuffham P. The Internet of Things: Impact and Implications for Health Care Delivery. **Journal of medical Internet research,** 22(11), 2020, e20135. https://doi.org/10.2196/20135

Khan Y.,Bin Mohd Su'ud M., Alam M.P., & Ahmad S.F. Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. Electronics, 12(1), 2022, 88. DOI: 10.3390/electronics12010088.

Kotha A. & Manohar K. A device-based interoperability as a service for IoMT devices. Journal of Ambient Intelligence and Humanized Computing,14, 2023, 1-12. https://doi.org/10.1007/s12652-023-04669-8

Koutras D, Stergiopoulos G., DasaklisT., Kotzanikolaou P., Glynos D., & Douligeris C. Security in IoMT Communications: A Survey. Sensors (Basel, Switzerland), 20(17), 2020, 4828. https://doi.org/10.3390/s20174828

Kumar V, Mahmoud M.S, Alkhayyat A, Srinivas J, Ahmad M, & Kumari A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. **The**

Journal of supercomputing, 78(14), 2022, 16167–16196. https://doi.org/10.1007/s11227-022-04513-4

Lim J. Scalable Fog Computing Orchestration for Reliable Cloud Task Scheduling. Applied Sciences, 11(22), 2021, 10996. DOI: 10.3390/app112210996.

Mamdiwar S.D, Shakruwala Z, Chadha U.,Srinivasan K., & Chang C.Y. Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring. Biosensors, 11(10), 2021, 372. https://doi.org/10.3390/bios11100372

Mazhar T, Malik A, Mohsan S.A.H., Y, Haq Li, I, Ghorashi S, Karim F, & Mostafa. S. M. (2023). Quality of Service (QoS) Performance Analysis in a Traffic Engineering Model for Next-Generation Wireless Sensor Networks. Symmetry,15. doi:10.3390/sym15020513

Mehmood G.,Khan M., Waheed A.,Zareei M. , Fayaz M., Sadad T.,Kama N., & Azmi A. An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network. Complexity. 2021. https://doi.org/10.1155/2021/6577492

Miranda E., Aryuni M., & Putra R. Mobile-Based Telemedicine Application during COVID-19 Pandemic (Case Study in Sawah Besar Community Health Center), 2021, 7-12. doi:10.1109/ICON-SONICS53103.2021.9617178

Mohamed Akram K, Sihem S, Okba K, & Harous S. IoMT-fog-cloud based architecture for Covid-19 detection. Biomedical signal processing and control, 76, 2022, 103715. https://doi.org/10.1016/j.bspc.2022.103715

Mohd Aman A.H., Hassan W.H., Sameen S., Attarbashi Z.S., Alizadeh, M. & Latiff L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. Journal of network and computer applications (Online), 174, 2021, 102886. https://doi.org/10.1016/j.jnca.2020.102886

Mubaraki A. A., Alrabie A. D., Sibyani A.K., Aljuaid R. S., Bajaber A. S., & Mubaraki M. A. Advantages and disadvantages of telemedicine during the COVID-19 pandemic era among physicians in Taif, Saudi Arabia. **Saudi medical journal,** 42(1), 2021, 110–115. https://doi.org/10.15537/smj.2021.1.25610

Nagajayanthi B. (2022). Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective. Wireless personal communications,123(4), 3661–3697. https://doi.org/10.1007/s11277-021-09308-z

Naqvi K., Markus E., Muthoni M., & Abu-Mahfouz A. (2022). A Critical Review of IoT-Connected Healthcare and Information Security in South Africa. In Advances in IoT, Industrial Informatics and Smart Applications, (pp. 739-746). doi:10.1007/978-981-16-4016-2_70

Nižetić S, Šolić, P, López-de-Ipiña González-de-Artaza D., & Patrono L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable

future. Journal of cleaner production, 2020, 274, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

Nwabueze C.,Eng M., Silas M., & Akaneme S. Wireless fidelity (Wi-Fi) broadband network technology: An overview with other broadband wireless networks. **Journal of Technology in Human Services,** 28(1), 2009, 71-78.

Onesimu A., Karthikeyan J., & Sei Y. An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT-based healthcare services. Peer-to-Peer Networking and Applications, 14(15), 2021. DOI: 10.1007/s12083-021-01077-7.

Onumanyi A. J, Abu-Mahfouz A. M. & Hancke G. P. Low Power Wide Area Network, Cognitive Radio and the Internet of Things: Potentials for Integration. Sensors (Basel, Switzerland), 20(23), 2020, 6837. https://doi.org/10.3390/s20236837

Osama M, Ateya A.A., Sayed M.S, Hammad.M, Pławiak P, Abd El-Latif A.A., & Elsayed R.A. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. Sensors (Basel, Switzerland), 23(17), 2023, 7435. https://doi.org/10.3390/s23177435-

Patra M., Sahoo B., & Turuk A. Smart Healthcare System Using Containerized Internet of Medical Things. In Handbook of Research on Smart Computing for Healthcare and Medicine, 2022. doi:10.4018/978-1-6684-4580-8.ch014

Pournik O, Mukherjee T, Ghalichi L & Arvanitis T.N. How Interoperability Challenges Are Addressed in Healthcare IoT Projects. Studies in health technology and informatics, 309, 2023, 121–125. https://doi.org/10.3233/SHTI230754

Rahi S., Munawar Khan M., & Alghizzawi. M. Factors influencing the adoption of telemedicine health services during COVID-19 pandemic crisis: An integrative research model. Enterprise Information Systems, 2020. https://doi.org/10.1080/17517575.2020.1850872

Rahman M.A., Victoros E., Ernest J., Davis R., Shanjana Y., & Islam M.R. Impact of Artificial Intelligence (AI) Technology in Healthcare Sector: A Critical Evaluation of Both Sides of the Coin. Clinical pathology (Thousand Oaks, Ventura County, Calif.), 17, 2024, 2632010X241226887. https://doi.org/10.1177/2632010X241226887

Ramalingam A., Dr Karunamurthy A, & Pavithra B. Impact of Artificial Intelligence on Healthcare: A Review of Current Applications and Future Possibilities. **Quing International Journal of Innovative Research in Science and Engineering,** 2(2), 2023, 37-49. doi:10.54368/qijirse.2.2.0005

Roy S, & Sarddar D. The Role of Cloud of Things in Smart Cities. **International Journal of Computer Science and Information Security (IJCSIS),** 14, 2016.

Sadhu P. K. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. Sensors, 22(15), 2022, 5517. https://doi.org/10.3390/s22155517

Sadhu P.K, Yanambaka V.P, Abdelgawad A., & Yelamarthi K. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. Sensors (Basel, Switzerland), 22(15), 2022, 5517. https://doi.org/10.3390/s22155517

Senthilkumar S., Poorana, & Subramani B. Study on IoT Architecture, Application Protocol and Energy needs. Biosensors, 2020, 8, 7-12.

Seth M., Jalo H., Högstedt A., Medin O., BjörneU. r, Sjöqvist B.A., & Candefjord S. Technologies for Interoperable Internet of Medical Things Platforms to Manage Medical Emergencies in Home and Prehospital Care: Protocol for a Scoping Review. JMIR research protocols, 11(9), 2022, e40243. https://doi.org/10.2196/40243

Shafiq M., Choi J.G., Cheikhrouhou O., & Hamam H. Advances in IoMT for Healthcare Systems. Sensors (Basel, Switzerland), 24(1), 2023, 10. https://doi.org/10.3390/s24010010

Shakeel T., Habib S., Boulila W., Koubaa A., Javed A.R., Rizwan M., Gadekallu T., & Sufiyan M. A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects. Complex & Intelligent Systems, 9, 2022. https://doi.org/10.1007/s40747-022-00767-w

Shrestha S., & Shakya S. Technical Analysis of ZigBee Wireless Communication. **Journal of Trends in Computer Science and Smart Technology,** 2, 2021, 197-203. doi:10.36548/jtcsst.2020.4.004

Singh A., Luhach A., Gao X.Z., Kumar S., & Sinha Roy D. Evolution of wireless sensor network design from technology centric to user centric: An architectural perspective. International Journal of Distributed Sensor Networks, 16, 2020. 1550147720949138. doi:10.1177/1550147720949138

Solimini R., Busardò F., Gibelli F., Sirignano A., & Ricci G. Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic. Medicina (Kaunas, Lithuania), 57, 2021. https://doi.org/10.3390/medicina57121314

Srivastava J., Routray S., Ahmad S., & Waris M.M. Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress. Computational intelligence and neuroscience, 2022, 7218113. https://doi.org/10.1155/2022/7218113

Taherdoost H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics,12 (8), 2023, 1901. https://doi.org/10.3390/electronics12081901

Ubaidullah M., & Makki Q. A Review on Symmetric Key Encryption Techniques in Cryptography. **International Journal of Computer Applications,** 2016, 147, 43-48. https://api.semanticscholar.org/CorpusID:64450272

Uslu B.C, Okay E, & Dursun E. Analysis of factors affecting IoT-based smart hospital design. Journal of cloud computing (Heidelberg, Germany), 2020, 9(1), 67. https://doi.org/10.1186/s13677-020-00215-5

Wagan S.A., Koo, Siddiqui J. I.F., Attique M., Shin D.R., & Qureshi N.M.F. Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. Journal of King Saud University - Computer and Information Sciences, 34(10), 2022, 9228-9251.

Appendices

Appendix A.: Visual Studio Environment

Visual Studio serves as the primary Integrated Development Environment (IDE) due to its powerful, integrated features:

- **Code Editing, Debugging, and Project Management**: Visual Studio's comprehensive tools streamline the development workflow, aiding in faster, more organized project execution.
- **Cross-Platform Development**: Visual Studio's support for both mobile and cloud components simplifies development across platforms, aligning with the IoMT solution's diverse requirements.
- **Ecosystem of Extensions and Integrations**: With a rich selection of plugins, Visual Studio enhances productivity by offering additional resources directly within the IDE.
- **Collaboration and Version Control**: Integration with GitHub supports version control and collaborative coding, allowing efficient teamwork and continuous code improvement.
- **Debugging and Profiling Tools**: Advanced tools assist in precise issue resolution, critical for the IoMT solution's complex data handling.

Appendix B: .NET Framework

The .NET Framework is central to achieving the project's goals of interoperability and security, offering:

- **Language Interoperability**: Multi-language support enables seamless integration of diverse solution components.

- **Extensive Libraries and Frameworks**: Pre-built libraries accelerate development and ensure reliability.
- **Scalability**: Known for supporting growth, .NET enables the solution to adapt to increasing demands and evolving requirements.
- **Security**: With built-in security features, .NET helps safeguard sensitive health data, ensuring compliance with healthcare standards.

Appendix C MAUI for Mobile Application

MAUI (Multi-platform App UI) was selected to deliver a cohesive mobile experience across platforms:

- **Cross-Platform Mobile Development**: MAUI supports a single codebase for all platforms, reducing development effort and ensuring consistency.
- **Single Codebase**: Developing one codebase for multiple platforms streamlines maintenance and promotes a unified user experience.
- **Integration with .NET**: Seamless integration with .NET allows the reuse of existing libraries and skills, enhancing development efficiency.
- **Adaptive UIs**: MAUI's adaptability to different screen sizes ensures a user-friendly experience across devices, from smartphones to tablets.

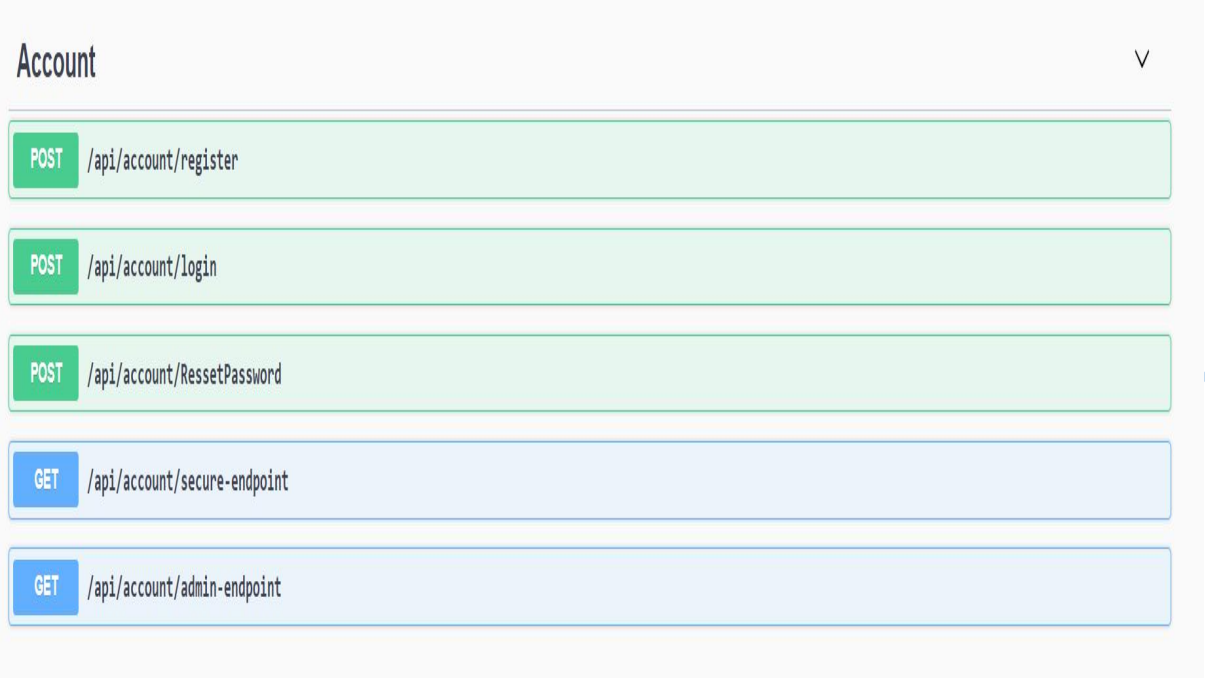
Appendix D: Account Management API

```
using Microsoft.AspNetCore.Mvc;
using System;
using System.Security.Claims;
using System.Threading.Tasks; // Import your AuthService
using Microsoft.AspNetCore.Authorization;
using Wasiu.Auth.Models;
using Wasiu.Authentication.Iservice;
using Wasiu.Telemedcine.Core.Models;
```

```
namespace Account.Controllers
{
   [Route("api/account")]
   [ApiController]
   public class AccountController : ControllerBase
   {
      private readonly IAuthService _authService;

      public AccountController(IAuthService authService)
      {
         _authService = authService ?? throw new ArgumentNullException(nameof(authService));
      }

      [HttpPost("register")]
      [AllowAnonymous] // Allow unauthenticated access
      public async Task<IActionResult> Register(RegisterRequestModel model)
      {
         try
         {
            // Implement your registration logic using the AuthService
            var additionalClaims = new[]
            {
               new Claim("CustomClaimType", "CustomClaimValue"), // Add custom claims as needed
            };

            var result = await _authService.RegisterUserAsync(model.Username, model.Password, additionalClaims);

            if (result.Success)
            {
               // Registration succeeded
               return Ok(new { Message = "Registration successful" });
            }

            // Registration failed
            return BadRequest(new { Message = result.ErrorMessage });
         }
         catch (Exception ex)
         {
            // Handle exceptions and return an error response
            return StatusCode(500, new { Message = "An error occurred while processing the request." });
         }
```

```
    }

    [HttpPost("login")]
    [AllowAnonymous] // Allow unauthenticated access
    public async Task<IActionResult> Login(LoginRequestModel model)
    {
        try
        {
            // Implement your login logic using the AuthService
            var token = await _authService.AuthenticateUserAsync(model.Username,model.Password);

            if (token != null)
            {
                // Login succeeded
                return Ok(new { Token = token });
            }

            // Login failed
            return Unauthorized(new { Message = "Invalid username or password." });
        }
        catch (Exception ex)
        {
            // Handle exceptions and return an error response
            return StatusCode(500, new { Message = "An error occurred while processing the request." });
        }
    }

    [HttpPost("RessetPassword")]
    [AllowAnonymous] // Allow unauthenticated access
    public async Task<IActionResult> RessetPassword(ResetPasswordModel model)
    {
        try
        {
            // Implement your login logic using the AuthService
            var token = await _authService.ResetPasswordAsync(model.Username, model.Password);

            if (token != null)
            {
                // Login succeeded
                return Ok(new { Token = token });
            }

            // Login failed
```

```
            return Unauthorized(new { Message = "Invalid username or password." });
        }
        catch (Exception ex)
        {
            // Handle exceptions and return an error response
            return StatusCode(500, new { Message = "An error occurred while processing the request." });
        }
    }

    [HttpGet("secure-endpoint")]
    [Authorize] // Requires authentication
    public IActionResult SecureEndpoint()
    {
        // This endpoint is accessible only to authenticated users
        return Ok(new { Message = "You have access to the secure endpoint." });
    }

    [HttpGet("admin-endpoint")]
    [Authorize(Roles = "Admin")] // Requires authentication and "Admin" role
    public IActionResult AdminEndpoint()
    {
        // This endpoint is accessible only to authenticated users with the "Admin" role
        return Ok(new { Message = "You have access to the admin endpoint." });
    }

    // Add more endpoints as needed, such as password reset, change password, etc.
  }
}
```



Appendix E: Device Management API

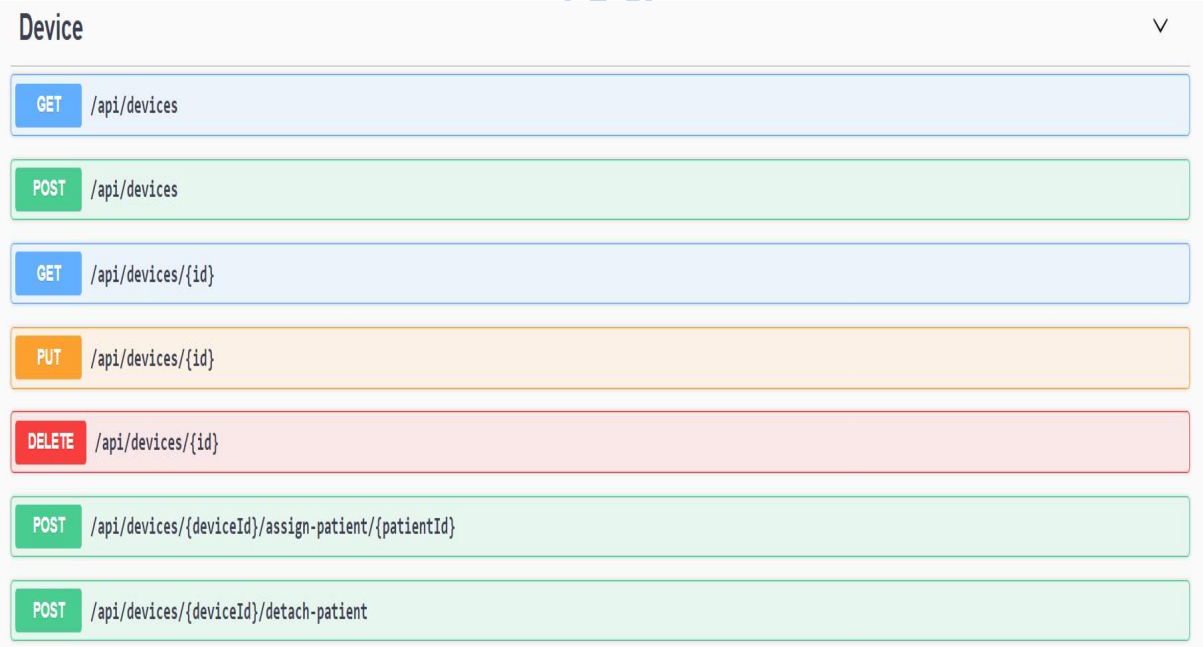
```
using Microsoft.AspNetCore.Mvc;
using System.Collections.Generic;
using System.Threading.Tasks;
using System;
using Wasiu.Telemedcine.Application.DTOs;
using Wasiu.Telemedcine.Core.Models;
using Wasiu.Telemedicine.Application.Interface;
using AutoMapper;
using Wasiu.Telemedicine.Application.Impkementation;

namespace Wasiu.Telemedcine.API.Controllers
{
   [Route("api/devices")]
   [ApiController]
   public class DeviceController : ControllerBase
   {
      private readonly IDeviceService _deviceService;
      private readonly IPatientService _petientService;
      private readonly IMapper _mapper; // Inject IMapper

      public DeviceController(IDeviceService deviceService, IMapper mapper,
IPatientService petientService)
      {
         _deviceService = deviceService;
         _mapper = mapper; // Inject IMapper
         _petientService = petientService;
      }

      // GET: api/devices
      [HttpGet]
      public async Task<ActionResult<IEnumerable<DeviceDto>>> GetDevices()
      {
         var devices = await _deviceService.GetAllDevicesAsync();
         var deviceDtos = _mapper.Map<IEnumerable<DeviceDto>>(devices);
         return Ok(deviceDtos);
      }

      // GET: api/devices/5
      [HttpGet("{id}")]
      public async Task<ActionResult<DeviceDto>> GetDevice(int id)
      {
         var device = await _deviceService.GetDeviceByIdAsync(id);

         if (device == null)
```

```
        {
            return NotFound();
        }

        var deviceDto = _mapper.Map<DeviceDto>(device);
        return Ok(deviceDto);
    }

    // POST: api/devices
    [HttpPost]
    public async Task<ActionResult<DeviceDto>> CreateDevice(DeviceDto deviceDto)
    {
        if (!ModelState.IsValid)
        {
            return BadRequest(ModelState);
        }

        var device = _mapper.Map<Device>(deviceDto);
        var createdDevice = await _deviceService.CreateDeviceAsync(device);

        var createdDeviceDto = _mapper.Map<DeviceDto>(createdDevice);

        return CreatedAtAction(nameof(GetDevice), new { id = createdDeviceDto.Id },
createdDeviceDto);
    }

    // PUT: api/devices/5
    [HttpPut("{id}")]
    public async Task<IActionResult> UpdateDevice(int id, DeviceDto deviceDto)
    {
        if (!ModelState.IsValid)
        {
            return BadRequest(ModelState);
        }


        if (id != deviceDto.Id)
        {
            return BadRequest();
        }
```

```
    var device = _mapper.Map<Device>(deviceDto);

    try
    {
        await _deviceService.UpdateDeviceAsync(id, device);
    }
    catch (Exception)
    {
        return NotFound();
    }

    return NoContent();
}

// DELETE: api/devices/5
[HttpDelete("{id}")]
public async Task<IActionResult> DeleteDevice(int id)
{
    var device = await _deviceService.GetDeviceByIdAsync(id);

    if (device == null)
    {
        return NotFound();
    }

    await _deviceService.DeleteDeviceAsync(id);

    return NoContent();
}
// POST: api/devices/{deviceId}/assign-patient/{patientId}
[HttpPost("{deviceId}/assign-patient/{patientId}")]
public async Task<IActionResult> AssignPatientToDevice(int deviceId, int patientId)
{
```

```
        // Check if the device and patient exist
        var device = await _deviceService.GetDeviceByIdAsync(deviceId);
        var patient =  _petientService.GetPatientById(patientId);

        if (device == null || patient == null)
        {
            return NotFound("Device or patient not found.");
        }

        // Associate the patient with the device (assuming you have such a method in your IDeviceService)
        bool result = await _deviceService.AttachDeviceToPatientAsync(deviceId, patientId);

        if (result)
        {
            return Ok("Patient assigned to the device successfully.");
        }
        else
        {
            return BadRequest("Failed to assign patient to the device.");
        }
    }
    // POST: api/devices/{deviceId}/detach-patient
    [HttpPost("{deviceId}/detach-patient")]
    public async Task<IActionResult> DetachDeviceFromPatient(int deviceId)
    {
        // Check if the device exists
        var device = await _deviceService.GetDeviceByIdAsync(deviceId);

        if (device == null)
        {
            return NotFound("Device not found.");
        }

        // Check if the device is currently assigned to a patient
        if (device.DeviceID == null)
        {
```

```
            return BadRequest("Device is not currently assigned to a patient.");
        }

        // Detach the device from the patient (assuming you have such a method in your IDeviceService)
        bool result = await _deviceService.DetachDeviceFromPatientAsync(device.DeviceID);

        if (result)
        {
            return Ok("Device detached from the patient successfully.");
        }
        else
        {
            return BadRequest("Failed to detach device from the patient.");
        }
    }


  }
}
```



Appendix F: Patient Device API

```
using AutoMapper;
using Microsoft.AspNetCore.Mvc;
using System.Threading.Tasks;
using System;
using Wasiu.Telemedcine.Application.DTOs;
using Wasiu.Telemedcine.Application.Interface;
using Wasiu.Telemedcine.Core.Models;

namespace Wasiu.Telemedcine.API.Controllers
{
   [ApiController]

   [Route("api/[controller]")]

   public class PatientDevicesController : ControllerBase
   {
      private readonly IPatientDeviceService _patientDeviceService;
      private readonly IMapper _mapper;


      public  PatientDevicesController(IPatientDeviceService  patientDeviceService,  IMapper
mapper)
      {
         _patientDeviceService = patientDeviceService;
         _mapper = mapper;
      }

      [HttpPost("assign")]
      public        async        Task<IActionResult>        AssignDeviceToPatient([FromBody]
PatientDeviceDto patientDeviceDto)
      {
         try
         {
            // Check if the device is already assigned to another patient
            var                                  existingAssignment                                =
_patientDeviceService.IsDeviceAssignedToPatientAsync(patientDeviceDto.DeviceId,patient
DeviceDto.PatientId);
            if (existingAssignment != null)
            {
               return BadRequest("Device is already assigned to another patient.");
            }

            // Unassign the device from any previous patient (if assigned)
```

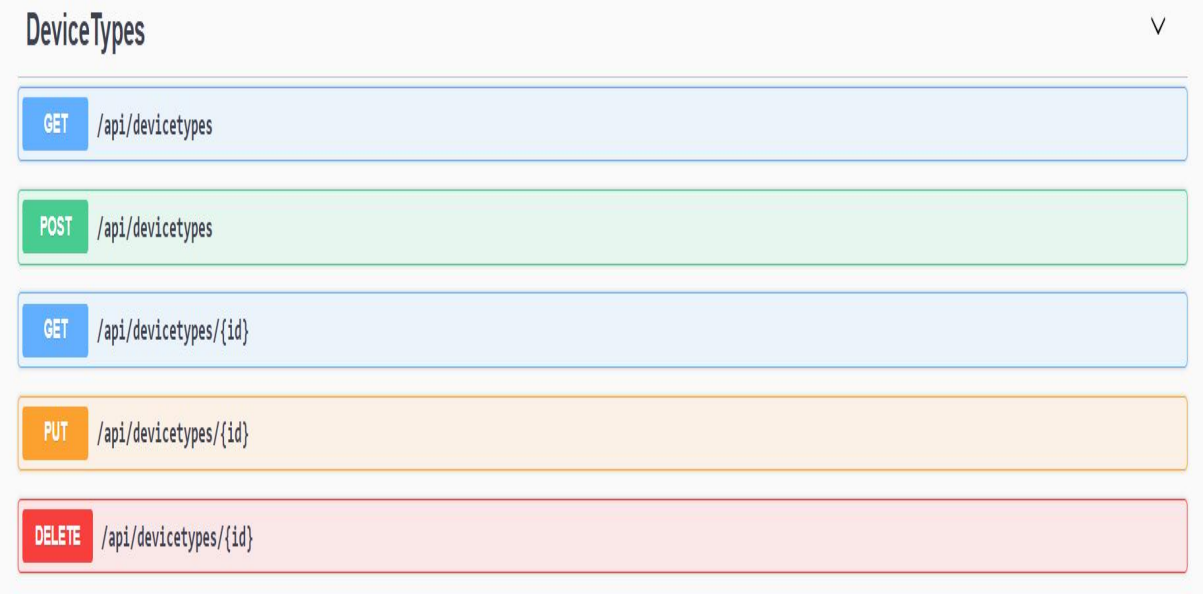
```
            var result = await _patientDeviceService.UnlinkDeviceFromPatientAsync(patientDeviceDto.DeviceId, patientDeviceDto.PatientId);

            var patientDevice = _mapper.Map<PatientDevice>(patientDeviceDto);
            var result1 = await _patientDeviceService.LinkDeviceToPatientAsync(patientDeviceDto.DeviceId, patientDeviceDto.PatientId);

            if (result == true)
            {
                return Ok();
            }

            return BadRequest(result);
        }
        catch (Exception ex)
        {
            return StatusCode(500, $"Internal server error: {ex.Message}");
        }
    }

    [HttpPost("unassign")]
    public async Task<IActionResult> UnassignDeviceFromPatient([FromBody] PatientDeviceDto patientDeviceDto)
    {
        try
        {
            var patientDevice = _mapper.Map<PatientDevice>(patientDeviceDto);
            var result = await _patientDeviceService.UnlinkDeviceFromPatientAsync(patientDevice.DeviceId, patientDeviceDto.PatientId);

            if (result == true)
            {
                return Ok(_mapper.Map<PatientDeviceDto>(result));
            }

            return BadRequest(result);
        }
        catch (Exception ex)
        {
            return StatusCode(500, $"Internal server error: {ex.Message}");
        }
    }
}
```

}

Appendix G: Device Type Management API

```
using AutoMapper;
using Microsoft.AspNetCore.Mvc;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;
using Wasiu.Telemedcine.Application.DTOs;
using Wasiu.Telemedcine.Application.Interface;
using Wasiu.Telemedcine.Core.Models;

namespace Wasiu.Telemedcine.API.Controllers
{
   [Route("api/devicetypes")]
   [ApiController]
   public class DeviceTypesController : ControllerBase
   {
      private readonly IDeviceTypeService _deviceTypeService;
      private readonly IMapper _mapper;

      public DeviceTypesController(IDeviceTypeService deviceTypeService, IMapper
mapper)
      {
         _deviceTypeService = deviceTypeService;
         _mapper = mapper;
      }

      [HttpGet]
      public async Task<ActionResult<IEnumerable<DeviceTypeDto>>> GetDeviceTypes()
      {
         try
         {
            var deviceTypes = await _deviceTypeService.GetAllDeviceTypesAsync();
            var deviceTypeDtos =
_mapper.Map<IEnumerable<DeviceTypeDto>>(deviceTypes);
            return Ok(deviceTypeDtos);
         }
         catch(Exception ex)
         {
            return BadRequest(ex.Message);
         }
      }

      [HttpGet("{id}")]
```

```
        public async Task<ActionResult<DeviceTypeDto>> GetDeviceType(int id)
        {
            var deviceType = await _deviceTypeService.GetDeviceTypeByIdAsync(id);

            if (deviceType == null)
            {
                return NotFound();
            }

            var deviceTypeDto = _mapper.Map<DeviceTypeDto>(deviceType);
            return Ok(deviceTypeDto);
        }

        [HttpPost]
        public async Task<ActionResult<DeviceTypeDto>> CreateDeviceType(DeviceTypeDto
deviceTypeDto)
        {
            var deviceType = _mapper.Map<DeviceType>(deviceTypeDto);
            await _deviceTypeService.AddDeviceTypeAsync(deviceType);
            var createdDeviceTypeDto = _mapper.Map<DeviceTypeDto>(deviceType);

            return Ok("Success");
        }

        [HttpPut("{id}")]
        public async Task<IActionResult> UpdateDeviceType(int id, DeviceTypeDto
deviceTypeDto)
        {

            var deviceType = _mapper.Map<DeviceType>(deviceTypeDto);
            await _deviceTypeService.UpdateDeviceTypeAsync(deviceType);

            return Ok("Success");
        }

        [HttpDelete("{id}")]
        public async Task<IActionResult> DeleteDeviceType(int id)
        {
            await _deviceTypeService.DeleteDeviceTypeAsync(id);
            return Ok("Success");
        }
    }
}
```



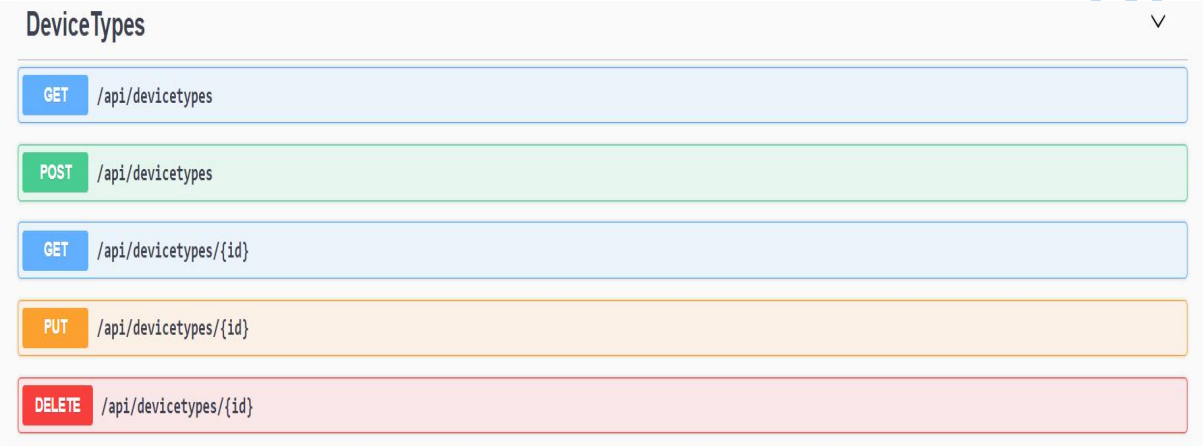
Appendix G: Device Manufacture API

```
using Microsoft.AspNetCore.Mvc;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;
using AutoMapper;
using Wasiu.Telemedcine.Core.DTOs.DeviceManufacturer;
using Wasiu.Telemedcine.Core.Models;
using Wasiu.Telemedcine.Application.Interface;

namespace Wasiu.Telemedcine.Web.Controllers
{
   [Route("api/device-manufacturers")]
   [ApiController]
   public class DeviceManufacturersController : ControllerBase
   {
      private readonly IDeviceManufacturerService _manufacturerService;
      private readonly IMapper _mapper;

      public                          DeviceManufacturersController(IDeviceManufacturerService
manufacturerService, IMapper mapper)
      {
         _manufacturerService = manufacturerService;
         _mapper = mapper;
      }
```

```
    [HttpGet]
    public async Task<IActionResult> GetManufacturers()
    {
        var manufacturers = await _manufacturerService.GetAllManufacturersAsync();
        var manufacturerDtos = _mapper.Map<IEnumerable<DeviceManufacturerDto>>(manufacturers);
        return Ok(manufacturerDtos);
    }

    [HttpGet("{id}")]
    public async Task<IActionResult> GetManufacturer(int id)
    {
        var manufacturer = await _manufacturerService.GetManufacturerByIdAsync(id);

        if (manufacturer == null)
        {
            return NotFound();
        }

        var manufacturerDto = _mapper.Map<DeviceManufacturerDto>(manufacturer);
        return Ok(manufacturerDto);
    }

    [HttpPost]
    public async Task<IActionResult> CreateManufacturer(DeviceManufacturerDto manufacturerDto)
    {
        var manufacturer = _mapper.Map<DeviceManufacturer>(manufacturerDto);
        await _manufacturerService.AddManufacturerAsync(manufacturerDto);

        // Return the created manufacturer with its assigned ID
```

```
        manufacturerDto = _mapper.Map<DeviceManufacturerDto>(manufacturer);
        return CreatedAtAction(nameof(GetManufacturer), new { id = manufacturerDto.Id },
manufacturerDto);
    }

    [HttpPut("{id}")]
    public async Task<IActionResult> UpdateManufacturer(int id, DeviceManufacturerDto
manufacturerDto)
    {
        if (id != manufacturerDto.Id)
        {
            return BadRequest();
        }

        var existingManufacturer = await
_manufacturerService.GetManufacturerByIdAsync(id);
        if (existingManufacturer == null)
        {
            return NotFound();
        }

        _mapper.Map(manufacturerDto, existingManufacturer);
        await _manufacturerService.UpdateManufacturerAsync(manufacturerDto);

        return Ok("Success");
    }

    [HttpDelete("{id}")]
    public async Task<IActionResult> DeleteManufacturer(int id)
    {
        var existingManufacturer = await
_manufacturerService.GetManufacturerByIdAsync(id);
        if (existingManufacturer == null)
        {
            return NotFound();
        }
```

```
            await _manufacturerService.DeleteManufacturerAsync(id);

            return Ok("Success");
        }
    }
}
```



Appendix I: Login Page for Mobile

```
<ContentPage xmlns="http://schemas.microsoft.com/dotnet/2021/maui"
             xmlns:x="http://schemas.microsoft.com/winfx/2009/xaml"
             BackgroundColor="#ffffff"
             x:Class="IOMTGate.LoginPage">

    <StackLayout Padding="20" Spacing="20">
        <!-- Add your login form elements here -->
        <Entry Placeholder="Username" x:Name="UsernameEntry" />
        <Entry Placeholder="Password" x:Name="PasswordEntry" IsPassword="True" />

        <Button Text="Login"
                BackgroundColor="#4CAF50"
                TextColor="#ffffff"
                FontSize="Large"
                CornerRadius="10"
                Clicked="OnLoginClicked"
                HorizontalOptions="FillAndExpand" />
        <Button Text="Reset Password"
                BackgroundColor="#007BFF"
                TextColor="#ffffff"
                FontSize="Large"
                CornerRadius="10"
                Clicked="OnResetPasswordClicked"
                HorizontalOptions="FillAndExpand" />

        <Button Text="Forgot Password?"
                BackgroundColor="#DC3545"
                TextColor="#ffffff"
                FontSize="Large"
                CornerRadius="10"
                Clicked="OnForgotPasswordClicked"
                HorizontalOptions="FillAndExpand" />
        <ActivityIndicator IsRunning="{Binding IsConnecting}" Color="Green" />
        <Label Text="Login ..." HorizontalOptions="Center" VerticalOptions="Center"/>
    </StackLayout>

</ContentPage>
```

Appendix J: Signup Page for Mobile

```
<ContentPage xmlns="http://schemas.microsoft.com/dotnet/2021/maui"
             xmlns:x="http://schemas.microsoft.com/winfx/2009/xaml"
             x:Class="IOMTGate.SignupPage"
             BackgroundColor="{DynamicResource PageBackgroundColor}"
             Title="Sign Up"
             Shell.FlyoutBehavior="Disabled">


    <StackLayout Padding="20" VerticalOptions="StartAndExpand">
        <Entry Placeholder="Surname" x:Name="SurnameEntry" />
        <Entry Placeholder="Firstname" x:Name="FirstnameEntry" />
        <Entry Placeholder="LastName" x:Name="LastNameEntry" />
        <DatePicker Date="{Binding BirthDate}" Format="D" />

        <StackLayout Orientation="Horizontal" VerticalOptions="StartAndExpand">
            <Label Text="Gender:" VerticalOptions="Center" />
            <StackLayout Orientation="Horizontal">
                <RadioButton GroupName="GenderGroup" x:Name="MaleRadioButton" />
                <Label Text="Male" VerticalOptions="Center" />
            </StackLayout>
            <StackLayout Orientation="Horizontal">
                <RadioButton GroupName="GenderGroup" x:Name="FemaleRadioButton" />
                <Label Text="Female" VerticalOptions="Center" />
            </StackLayout>
        </StackLayout>

        <Entry Placeholder="Email" x:Name="EmailEntry" />
        <Entry Placeholder="Phone" x:Name="PhoneEntry" />
        <Entry Placeholder="Address" x:Name="AddressEntry" />

        <!-- State and Local Government (Cascaded Dropdowns) -->
        <Picker x:Name="StatePicker" Title="Select State"
SelectedIndexChanged="OnStateSelectedIndexChanged">
            <!-- ... -->
        </Picker>

        <Picker x:Name="LocalGovtPicker" Title="Select Local Government"
IsEnabled="True">
            <!-- ... -->
        </Picker>

        <Button Text="Sign Up" Clicked="OnSignUpClicked" />
    </StackLayout>
</ContentPage>
```

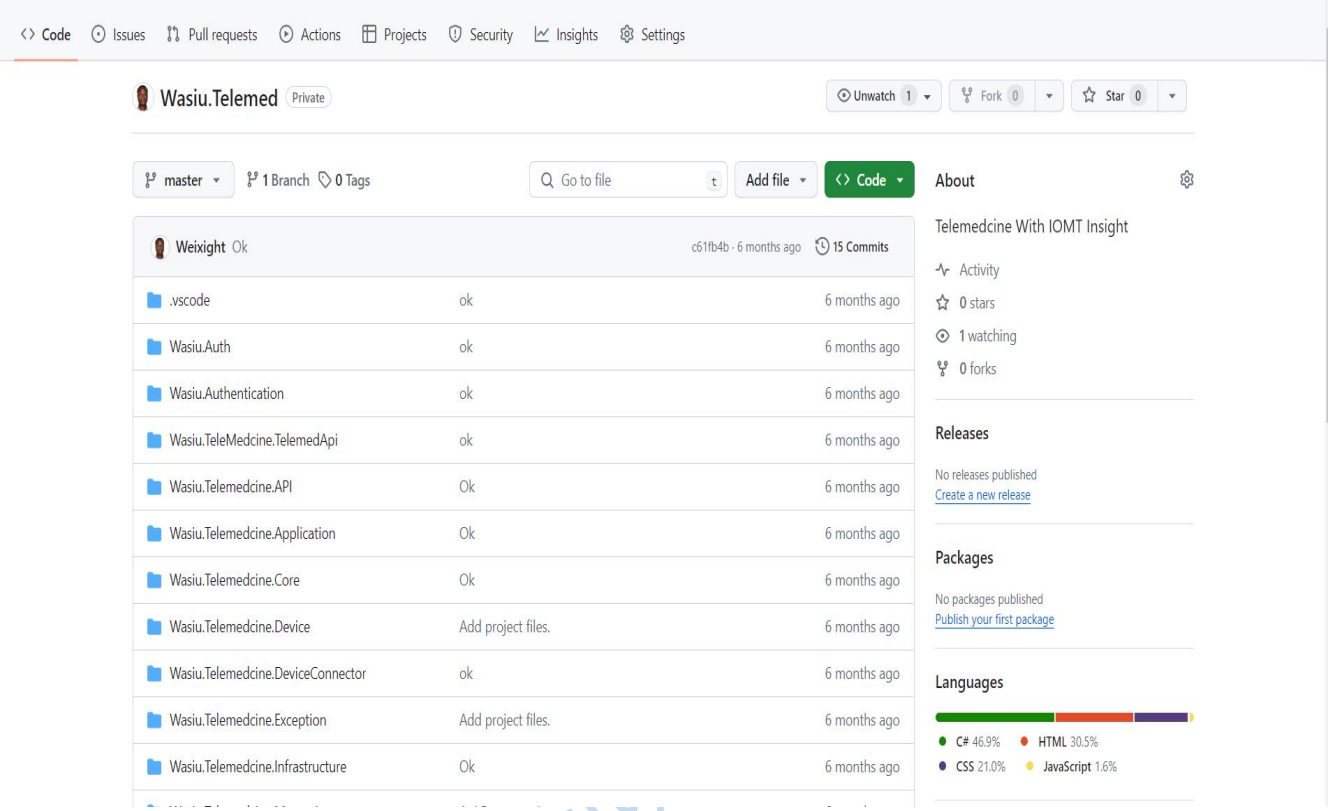
Appendix K: Device Registration Page for Mobile

```
<?xml version="1.0" encoding="utf-8" ?>
<ContentPage xmlns="http://schemas.microsoft.com/dotnet/2021/maui"
             xmlns:x="http://schemas.microsoft.com/winfx/2009/xaml"
             xmlns:d="http://schemas.microsoft.com/dotnet/2021/maui/design"
             xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
             mc:Ignorable="d"
             BackgroundColor="#ffffff"
             x:Class="IOMTGate.DevicesPage">

    <StackLayout>
        <!-- Section for Adding a New Device -->
        <StackLayout Padding="20" BackgroundColor="#f0f0f0">
            <Label Text="Add a New Device" FontSize="Subtitle" />

            <!-- Add your form or input elements here for adding a new device -->
            <!-- Example: -->
            <Entry Placeholder="Device Name" x:Name="DeviceNameEntry" />
            <!-- Manufacturer Picker -->
            <Picker x:Name="ManufacturerPicker" Title="Select Manufacturer"
SelectedIndexChanged="OnManufacturerSelectedIndexChanged">
                <!-- Populate the Manufacturers in code-behind -->
            </Picker>

            <!-- Model Picker -->
            <Picker x:Name="ModelPicker" Title="Select Model">
                <!-- Populate the Models based on selected Manufacturer in code-behind -->
            </Picker>

            <Button Text="Add Device" Clicked="OnAddDeviceClicked" />
        </StackLayout>

        <!-- Device List -->
        <ListView x:Name="DevicesListView" ItemsSource="{Binding Devices}">
            <ListView.ItemTemplate>
                <DataTemplate>
                    <ViewCell>
                        <!-- Customize the appearance of each device in the list -->
                        <SwipeView>
                            <SwipeView.RightItems>
                                <SwipeItems>
                                    <SwipeItem Text="View" IconImageSource="view_icon.png"
Command="{Binding Source={x:Reference DevicesListView},
Path=BindingContext.ViewCommand}" CommandParameter="{Binding .}" />
```

```
                        <SwipeItem Text="Update" IconImageSource="update_icon.png"
Command="{Binding Source={x:Reference DevicesListView},
Path=BindingContext.UpdateCommand}" CommandParameter="{Binding .}" />
                        <SwipeItem Text="Delete" IconImageSource="delete_icon.png"
Command="{Binding Source={x:Reference DevicesListView},
Path=BindingContext.DeleteCommand}" CommandParameter="{Binding .}" />
                    </SwipeItems>
                </SwipeView.RightItems>

                <StackLayout Padding="15">
                    <Label Text="{Binding DeviceName}" FontSize="Medium" />
                    <!-- Add more labels or controls to display other device information -->
                </StackLayout>
            </SwipeView>
        </ViewCell>
    </DataTemplate>
</ListView.ItemTemplate>
</ListView>
</StackLayout>
</ContentPage>
```

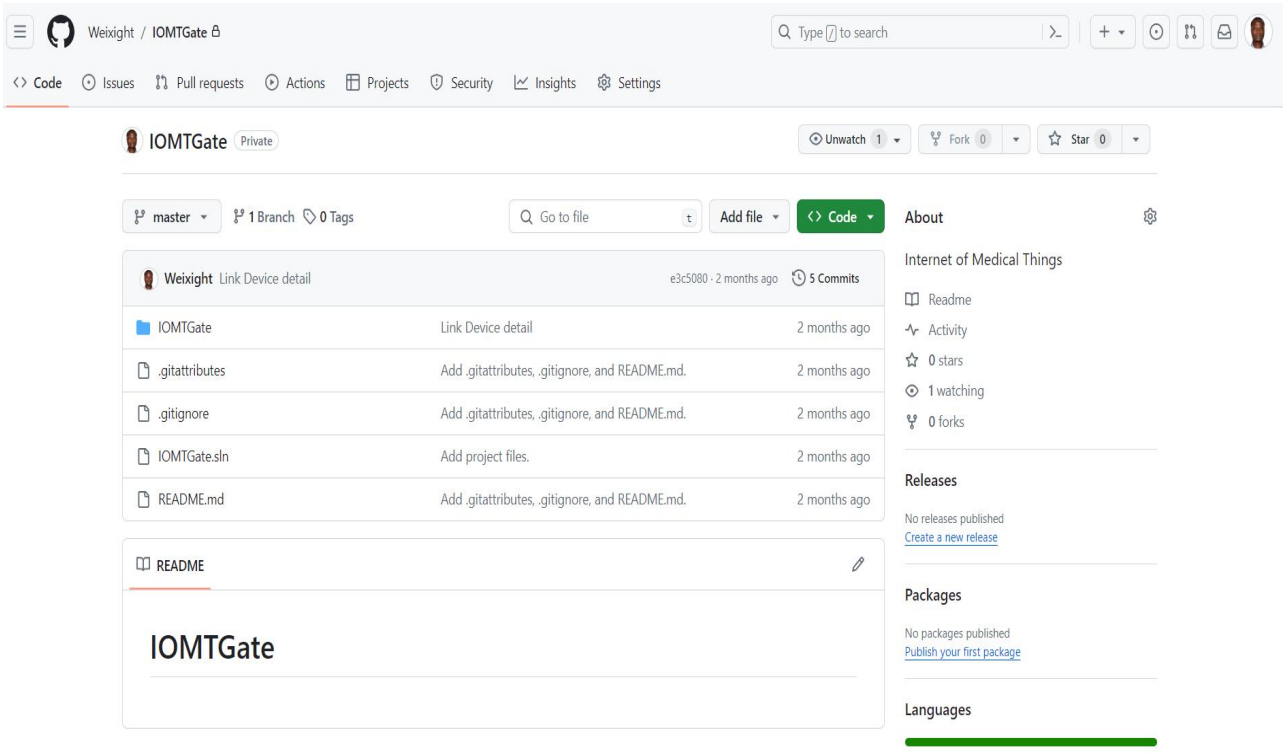
Appendix L: Complete Source Code on Git

https://github.com/Weixight/Wasiu.Telemed



Appendix M Complete Source Code for Mobile on Git

https://github.com/Weixight/IOMTGate



Bio-data

A. Personal Data:

Name:	Wasiu Olakayode OLAYINKA
Marital Status:	Married
Nationality:	Nigeria
Date of Birth:	30th October, 1981
State of Origin:	Oyo State
Local Government Area:	Akinyele
Sex:	Male
Contact Address:	121, Olatunji Street, Ojota lagos.
Phone:	08062-470-358, 08086900265
E-Mail:	weixight1@yahoo.com

B. Education Background

Lead City University, Ibadan Oyo State, till date, (MSc Computer Science)

Ladoke Akintola University of Technology, Ogbomosho, Oyo, State, 2011 (PGD Computer Science)

Lagos State Polytechnic, Ikorodu, Lagos State, 2006 -2008 (HND Computer Science)

Lagos State Polytechnic, Ikorodu, Lagos State, 2002 -2005 (OND Computer Science)

Ikolaba High School, Agodi GRA, Ibadan, Oyo State 1992- 1998 (SSCE and Olevel)

C. Work Experience with Dates

Knight Frank - Lagos, Nigeria (IT Support, 2023)

Lagos state public service staff development center (IT Support 2009- 2010)

Softlab technologies limited (Senior Software Developer 2012 to 2018)

ALPHABETA CONSULTING LLP (Senior Software Developer 2018 – 2022)

Alliance Consulting and Digital Services (Senior Software Developer 2022 – Till Date)

Softlab Technology Limited (Consultant 2022 – Till Date)

Agricgate Nigeria Limited (Consultant 2022 – Till Date)

Gaf Homes and Properties Nigeria Limited (Consultant 2023 – Till Date)

F. Public Journal and Articles

1. To implement quality assurance in an Agile software development process, a team composed of members from Babcock University's Software Engineering Department and the Department of Computer Science within the Faculty of Basic Science has been formed. The team includes Wunmi AJAYI, OLAYINKA Wasiu Olakayode, Fasina Temilade, and Mariam Gbadegesin. They can be contacted via email at wumiajayi1@yahoo.com, weixight1@yahoo.com, temiladefasina@gmail.com, and mariamgbadegesin@gmail.com, respectively.

H. Referees

1. **Mr. Saheed Adeniji**
   Managing Director Softlab Technologies Limited
   +234 706 913 5166
2. **Adetayo Adeniran**
   Head of Network and Infrastructure
   Global Oil Service Limited
   +234 802 343 5816
3. **Dr. Adewumi Ademola**
   Managing Director
   Axtury Nigeria Limited
   +234 802 226 1176

---------- ----------

Signature Date

The University Compliance Certification

This is to certify that this thesis by Wasiu Olakayode OLAYINKA with Matriculation Number LCU/PG/002846 in department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo state is in full Compliance with the University's format and styles.

---------- ----------

Signature Date