Blockchain Enabled Secure IoMT Framework

Submitted By

Panchal Barkha

22MCES07

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF TECHNOLOGY, INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2024

Blockchain Enabled Secure IoMT Framework

Major Project - II

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering (Cyber Security)

Submitted By

Panchal Barkha

(22MCES07)

Guided By

Dr. Jitendra Bhatia

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF TECHNOLOGY, INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2024

Certificate

This is to certify that the major project entitled "**Blockchain Enabled Secure IoMT Framework**" submitted by **Panchal Barkha (Roll No: 22MCES07)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (cyber Security) of Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-II, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Jitendra 22/05/24

Dr.Jitendra Bhatia
Guide & Associate Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr.Vijay Ukani
Associate Professor,
Coordinator M.Tech - CSE (Cyber Security)
Institute of Technology,
Nirma University, Ahmedabad

Bhavsar

Dr. Madhuri Bhavsar
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr Himanshu Soni
Director,
School of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Panchal Barkha**, Roll. No.**22MCES07**, give undertaking that the Major Project entitled "**Blockchain Enabled Secure IoMT Framework**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering (Cyber Security)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place:

Endorsed by

Dr. Jitendra Bhatia

(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Jitendra Bhatia**, Associate Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continual support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank **Dr. Madhuri Bhavsar**, Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. Himanshu Soni**, Hon'ble Director, School of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

Panchal Barkha

22MCES07

Abstract

With its incredible efficiency, the Internet of Things (IoT) in particular is transforming care for patients and healthcare operations. The medical industry has seen firsthand how this state-of-the-art equipment can change things. The incorporation of sensing into IoT devices facilitates seamless connectivity and the gathering of essential data required for patient monitoring and treatment optimization. Numerous medical devices, including wheelchairs, nebulizers, and oxygen pumps, can be monitored in real time using connected sensors. The gathering of vital signs, prescription data, diagnoses for patients, and medical history may be made possible by this integration. Strong security measures are required to guarantee privacy and confidentiality of patients as worries about the safety of this private health information have surfaced. This research proposes a blockchain, software defined networking (SDN) and artificial intelligence (AI) for offering security measures for medical IoT data. Medical IoT data is classified into two classes: attack (1) and normal (0), using a variety of machine learning (ML) classifiers, such as support vector machine (SVM), random forest (RF), and K-Nearest neighbor (KNN). We discuss the solution of our literature is based on the security mechanism for IoMT framework. This research work tackle these challenges and porposed a solution for healthcare IoT. Furthermore, other performance measures are taken into consideration evaluation, including accuracy, precision, recall and F1 score. The detection model using SVM obtained 75.3%, RF is 75.9% and K-NN is 84.3%. The K-NN gets the greatest accuracy among all ML classifiers.

Abbreviations

IoMT	Internet of Medical Things.
AI	Artificial Intelligence.
SDN	Software Defined Networking.
ML	Machine Learning.
SVM	Support Vector Machine.
RF	Random Forest.
K-NN	K-Nearest neighbor.
IoT	Internet of Things.
BLE	Bluetooth.
MQTT	Message Queuing Telemetry Transport.
HTTP	Hypertext Transfer Protocol.
EHRs	Electronic Health Records.
IPFS	InterPlanetary File solution.
DDoS	Distributed Denial of Service.
HIS	Healthcare Information System.
PUF	Physically Unclonable Functions.
AC	Accuracy.
PR	Precision.
SC	Smart Contract.
mHealth	Mobile Healthcare.

Contents

List of Figures

Chapter 1

Introduction

Recently, a variety of technology innovations make people lives easier, including autonomous vehicles, smart homes, smart healthcare, and smart agriculture. Medical devices and the IoT are combined to form the IoMT. Healthcare professionals will be able to connect and monitor every medical device through the IoMT. As it develops, this provides faster and less expensive medical care. Technology has recently made significant strides in the development of IoT systems enabling the design of low power and inexpensive sensors. In order to provide remote patient monitoring these sensors have become increasingly popular in recent years eliminating the necessity for clinicians to be physically present in the field. Numerous medical applications including early detection, continuous tracking, and medical emergencies can be effectively supported by recent developments in the IoT and wireless communications. The quick identification of dangerous emergency cases through the application of safe and useful approaches potentially save healthcare expenses and lessen the need for carers in real time [4]. The development of clever decision making strategies can facilitate early interventions that lead to better health outcomes and may even save community members lives. Continuous monitoring of community members vital signs which wearable sensors may record is necessary to meet these objectives. The citizens of these smart communities can then receive effective remote healthcare communication to receive surveillance and diagnosis services from healthcare providers. Any danger to the security of these systems might result in a major issue such forcing a false diagnostic or postponing the contact. [1]. Secure IoMT frameworks are a developing discipline that includes topics like as AI-powered protocols for communication, prediction security frameworks and the integration of emerging tech-

nologies like SDN and Blockchain. [2]These frameworks provide increased security for IoMT applications and set the stage for a healthcare environment that is more adaptable and robust. The application of explainable AI models, patient focused control over health data and the ethical consequences of AI will be the main areas of future study in this sector to enhance IoMT security visibility and confidence. The multidisciplinary character of IoMT application security is illustrated by these many approaches which also highlight the necessity of cooperation between the information security, medical care, and technology sectors to guarantee the long term sustainability of confidential networked healthcare systems.

As of right now monitoring health remotely requires IoMT. The majority of wearable sensor applications include distant data gathering that is sent to the cloud for additional processing in the moment analysis and monitoring [7]. Using data from many IoT research projects this paper looks at the various applications of IoMT in medicine to examine how these have improved patient outcomes. Improving the results for patients and engagement is one area where IoMT transformative potential is most apparent. Wearable technology with sensors can track vital signs, level of exercise and adherence to medicine giving a more comprehensive view of a person health [3]. IoMT technology allows for remote patient monitoring which helps doctors monitor long-term conditions and intervene fast when abnormalities arise. Moreover IoMT facilitates the shift in healthcare from a reactive to a proactive approach by utilizing AI powered algorithms and predictive analytics to identify potential health issues before they manifest clinically. The IoMT is expanding rapidly and raises a number of concerns including privacy, security and connection. The interconnection of healthcare equipment networks makes them more vulnerable to hackers. It becomes essential to protect the privacy and security of personal health information which calls for the installation of strong security measures and well established procedures. IoMT devices produce a great deal of personal health data which highlights the need for strict consent and data protection procedures and poses privacy issues.[5]

1.1 Motivation

IoMT exploration is driven by its potential to transform healthcare through faster, more affordable medical care delivery and the ability to monitor health remotely. The use of wearable sensors is essential for collecting data that will be uploaded to the cloud and used to improve patient outcomes. Introducing cutting-edge technologies like AI, blockchain and SDN seeks to solve significant issues, improve device functionality and ensure the safe and effective operation of IoMT systems. The rising use of technology in healthcare, together with the sophistication of cyber threats, has prompted the creation of a safe framework for IoMT applications. Sensitive medical data must be protected from potential security breaches since IoMT promises revolutionary improvements in patient care and treatment. The increasing number of medical devices that are linked, along with the intrinsic weaknesses in IoMT designs, highlight the necessity of having a strong security framework. The goal of this study is to solve these issues, strengthen the IoMT ecosystems resilience, and help realise the vision of a future for linked healthcare that is safe, effective and privacy preserving.

1.2 Research Contribution

The main contributions of the research work are as follows:

- To provide a blockchain and AI based safe data exchange platform for the medical IoT.
- We provided a thorough overview of wearable technology, BANs and the digital healthcare system in our research work on smart healthcare technologies.
- The proposed approach uses many ML classifiers, including SVM, RF and K-NN to categorize medical IoT data into attack (1) and normal (0) classes. Additionally, the proposed method evaluates the issue of data imbalance and uses a sampling mechanism to balance the dataset.
- An IPFS-based blockchain technology is employed to enhance data security immutable blocks provide safe data storage for Medical IoT and smart contracts ensure data validation.

- This research addressed a variety of factors including accuracy, precision, recall and F1Score to evaluate the performance of the proposed system.
- Finally, we outlined a various open issues and future research directions for smart healthcare technology.

1.3 Organization

The flow of this research work is as follows. Section II provides the literature work based on secure IoMT framework. Section III provides the various open issues and research challenges in smart healthcare. Section IV discusses the proposed approach for smart healthcare. In Section V provides an overview and experimental setup of the proposed approach presented. Finally, Section VI offers the summary conclusion and future work.

1.4 Background

This section provides a background on IoMT in smart healthcare system. Different types of protocols. Security threats in recent case studies will be introduced in this part.

1.4.1 IoMT Smart Healthcare System

The IoMT has been driving the IoT rapidly in the healthcare industry. This emerging sector is bringing in a new age of smart healthcare systems and has inspired a great deal of interest and enthusiasm. IoMT provides a range of cutting-edge services that enable patients to perform monitoring and diagnostics from the comfort of their own homes by utilizing IoT technology. With the easy integration of sensors and linked devices people may now take an active role in managing their own healthcare going beyond routine visits to the hospital or clinic. [10] This revolutionary change brings in a period of patient-centric healthcare delivery by improving access to treatment and encouraging preventative and personalized care strategies.

IoMT devices connect to cloud systems so that collected data may be saved and examined. Healthcare IoT is another name for IoMT. The technique of using IoMT technology to remotely monitor patients while they are their homes is known as telemedicine. IoMT uses remote diagnostic technologies and video conferencing to facilitate online discussions between clients and medical professionals. This makes it easier for those who reside in

rural or economically isolated areas to obtain healthcare services and lessens the requirement for in person visits. Vital indicators such as blood pressure, oxygen saturation and heart rate may be remotely monitored with IoMT devices [6]. This enables medical personnel to keep an eye on their patients health in real time and act quickly to address any potential problems.

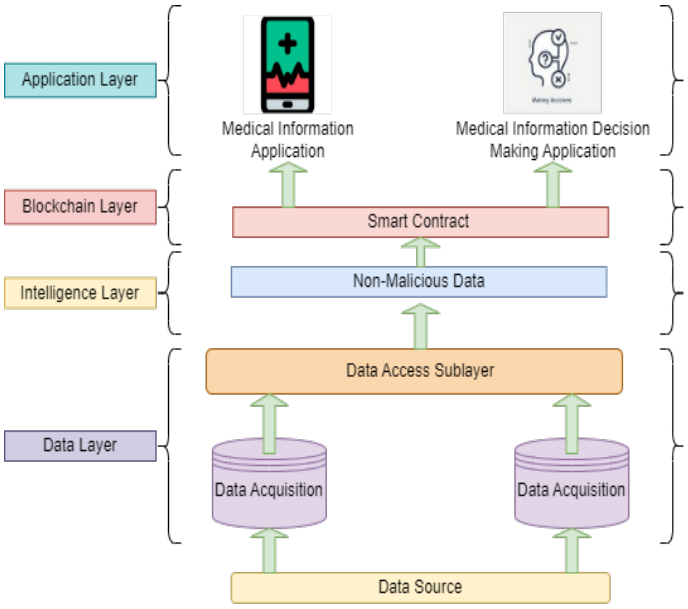

Figure 1.1: Working of IoMT in Smart Healthcare[9]

1.4.2 IoMT Protocols

The IoMT in smart healthcare systems is made up of several sensors each with unique communication features and protocols [8]. Heart sign tracks, wearable health trackers, smart medical gadgets and environmental sensors are some examples of these sensors. Various IoMT devices transmit data using different protocols such as HTTP/HTTPS, MQTT, low-energy Bluetooth (BLE), zigbee, wireless (3G/4G/5G) and Wi-Fi. These protocols provide the simple transmission of vital health data across IoMT devices allowing for remote monitoring, real time diagnosis and customised healthcare delivery that enhances patient outcomes and boosts overall industry efficiency.

1. **MQTT**: A lightweight communications protocol called MQTT (Message Queuing Telemetry Transport) was developed for IoT applications like intelligent medical equipment. MQTT makes it easier to make decisions, gather data, and analyze it by enabling effective, actual time interaction between medical equipment, sensors, and cloud-based apps.

2. **HTTP**: The Hypertext Transfer Protocol, also known as HTTP, including it secured variation HTTPS are commonly used by web-based healthcare apps, servers, and clients to facilitate communication. HTTP/HTTPS protocols enable secured online use of healthcare systems, electronic health records (EHRs) and various other web-based healthcare services.

1.4.3 Security Threats

Physical attacks and network-oriented threats are two types of specialized security risks that might affect sensor equipment. Dangers like data interception, unauthorized access, and denial-of-service attacks that target sensor communication channels are all considered network-oriented threats. On the other hand physical device attacks involve acts that risk the integrity and operation of sensors, such as tampering, theft, or environmental risks.

- Physical Devices

    1. **Tampering** : Device integrity and security may be compromised by physical tampering. In order to alter data readings, interfere with device operation, or obtain unauthorized access to private data, attackers may tamper with the hardware, sensors, or connections of the device.
    2. **Jamming** : On networks like Wi-Fi and Bluetooth, jamming attacks have the power to prevent or stop transmission entirely. This may cause the systems that depend on the internet to stop working and lose connectivity.

- Network Oriented Threats

    1. **DoS** : Through heavy traffic or request flooding, DoS attacks try to tamper with sensor device or network infrastructure regular operation, resulting in data loss, system failures, or service downtime.
    2. **MITM** : Attackers can change or generate data packets, steal private data, or affect device behaviour covertly by intercepting and changing communication between sensor devices and network servers.
    3. **Packet Sniffing** : Attackers may find weaknesses, extract sensitive data, or gain unauthorized access to the network by using packet sniffing techniques to record and analyze network traffic between sensor devices and network servers.

- Recent News Based on Case Studies

    1. In Feb 2022, A ransomware assault at Morley businesses, a third-party supplier of business services to Fortune 500 businesses, including those in the medical field, exposed approximately 521,000 individual records.
    2. The Shields Healthcare Groups network server was compromised by an unknown cyberattacker between March 7, 2022, to March 21, 2022. On March 18, the hackers presence activated a security alert, however, at the time of the warning investigation, data compromise was not established.
    3. Between Jan 18, 2022, and Feb 24, 2022, cybercriminals gained unauthorized access to ARcare's computer systems and utilized it to examine and steal confidential client information. On April 4, it was discovered that some of the stolen information was accessible online. It is possible that the incident was a ransomware attack because of this behavior pattern, which makes stolen material public shortly after a breach.

Chapter 2

Literature Survey

A literature review offers a thorough summary of all the studies and publications that have already been done on a certain subject. It provides an overview of the state of knowledge in a certain topic by summarising important discoveries, research techniques, and gaps in the body of literature. Researchers may use this poll to better understand the background of their work, the development of ideas, and the areas in which their own research might advance or add to current knowledge.

Mian Ahmad et al. [11] P2DCA, a strong framework created to handle privacy issues in IoMT applications, is introduced in this study. The system guarantees secure data gathering and analysis, protecting sensitive health information while permitting important insights by including cutting-edge privacy-preserving techniques. In order to improve the security and confidentiality of healthcare data in linked medical settings, researchers and practitioners may benefit greatly from our study, which emphasises the importance of privacy issues in the rapidly changing IoMT scenario.

Shahzana et al. [12] propose Software-Defined Networking orchestration as a tactical countermeasure against the dynamic and ever-evolving cyber threats that impact IoMT devices and systems. The study provides practitioners and academics in the domains of computer communications and healthcare cybersecurity with useful information by providing a flexible and centralized approach for enhancing IoMT security through the use of SDN.

Lanfang et al. [13] provide a detailed analysis of this integration's application, technology, and design. The research on the interface between edge-cloud computing and artificial intelligence offers valuable insights into the improved features and possible applications within the IoMT ecosystem. Grants access to a priceless resource for information on edge-cloud computing, AI, and IoMT's possible cooperation in the creation of medical technologies and applications.

Soneila et al. [14] proposed architecture creates an intelligent and adaptable detection of malware system for Internet of Medical Things (IoMT) situations by fusing SDN capability with Deep Learning approaches. The goal of this hybrid approach is to offer a practical response to the ever-changing problems that healthcare systems cyberthreats present. The utilization of cutting-edge technology for IoMT security is addressed in this article, which is helpful given the growing worries regarding cybercrime in the health care sector.

In order to improve the functionality and effectiveness of IoMT systems, Khalid et al. [15] provide an approach that blends Big Data, SDN and ML techniques. The suggested approach seeks to offer a complete solution for real-time management and analysis of massive amounts of data produced by medical devices by using these technologies. This work highlights the potential of multidisciplinary methods in the realm of electronics and healthcare technology, and is especially beneficial in the context of enhancing the performance and scalability of IoMT systems.

Prabhat et al. [16] the system successfully detects and mitigates cyberattacks by utilizing fog-cloud architecture and ensemble learning techniques. The authors stress how important it is to combine different learning models in order to increase the durability and accuracy of cyber attack detection in IoMT scenarios. Within the context of Computer Communications, the proposed framework contributes to the growing body of research on the security of networked medical devices and systems in the quickly evolving field of healthcare technology.

In order to address security issues in IoMT situations, Mohammad et al. [17] the pro-

tocol applies AI techniques. Protecting sensitive health data transmitted over insecure networks is imperative, and the authors recommend ASCP-IoMT as a solution. Among the protocols security features are key agreement, authentication, and the use of AI for increased security. This work adds to the subject of secure communication in IoMT and is significant since it focuses on medical services, security requirements, and the usage of AI.

Sahshanu et al. [18] go into great depth on IoMT, including the way it works with medical equipment and how it might affect healthcare. The authors address significant e-healthcare issues by evaluating cutting-edge technologies such as SDN, Blockchain, AI and Physically Unclonable Functions (PUF). They stress how important it is to have better performance, accuracy, privacy, and security. The paper is an asset for understanding IoMT architecture and its revolutionary impact on healthcare systems. It contains case examples that illustrate practical implementations.

Panagiotis et al. [19] the authors provide a cutting-edge method for modelling, identifying, and reducing risks against industrial healthcare systems that blends reinforcement learning with SDN. The goal of this multidisciplinary approach is to improve the security and resilience of healthcare systems in industrial environments while offering practitioners and academics in the fields of cybersecurity and industrial informatics useful new perspectives.

The framework aims to prevent and predict cyberattacks by utilising deep learning, machine intelligence, and blockchain technologies, as reported by Bandar, M. et al. [20]. The study provides a predictive security architecture for preventative defence along with an innovative approach to resolving security challenges with IoMT systems. The results and possible contributions of this study may offer important new perspectives on how to create reliable security solutions for IoMT technology.

Fazlullah et al. [21] the paper focuses on using fog-cloud architecture and ensemble learning approaches to identify cyberattacks in IoMT networks with high reliability. In the context of industrial informatics, their suggested secure ensemble learning-based methodology seeks to develop methods for detecting and preventing cyber threats.

Sotirios et al. [22] the investigates the use of AI technology to improve IoMT device security. The authors explore a number of topics, such as the use of AI to medical IoT threat detection, anomaly identification, and general security reinforcement. Through a detailed analysis of recent developments and future uses in the field of healthcare technology, this paper provides insightful information about how AI might be integrated to strengthen the security elements of IoMT.

Table 2.1: Literature Review Table

Author	Year	Key Contribution	Attack	ML Techniques	Limitations/Future Scope
Mian Ahmad et al.[11]	2019	A neural network analysis and cluster-based partitioning system for effective privacy-preserving data collecting and analysis for IoMT applications.	Replay attack	K-NN, SVM, ANN	Based on simulation findings, more improvements to the P2DCA framework to safeguard the privacy of visual contents in recorded videos.
Shahzana et al.[12]	2020	Complicated multivector malware botnets quickly and effectively, offer a hybrid DL-driven SDN-enabled IoMT framework that makes use of CNN and cuDNNLSTM.	DoS, DDoS, Data-Injection	CNN, DNN, LSTM	Hybrid DL-driven architectures in developing computational paradigms and IoT ecosystems.
Lanfang et al.[13]	2020	Processing large amounts of medical data and delivering high-quality healthcare services may be addressed by using cloud, edge, and AI computing.	Dos, MITM	Clustering, CNN	Need to reduce energy usage, protect patient privacy and secure medical data a major problem for the rapidly changing medical industry.
Soneila et al.[14]	2021	Provide a highly scalable hybrid deep learning driven SDN-enabled platform that can identify sophisticated IoMT malware quickly and effectively.	Malware	CNN, LSTM	Creation of hybrid deep learning systems to improve security protocols in developing IoT networks.
Khalid et al.[15]	2021	Predicting network resource usage and enhancing sensor data transmission efficiency in IoMT applications with machine learning and SDN-enabled security.	Malware	CNN, LSTM	Boosting accuracy by applying deep learning techniques to IoT services and increasing scalability by adding multiple controllers.
Prabhat et al.[16]	2021	A fog-cloud architecture driven cyber attack detection method for IoMT networks based on ensemble learning that achieves high detection rates and accuracy using a realistic dataset.	Ransomware, DoS	DT, Naive Bayes, RF	Creating a prototype of the suggested model for real-time verification in a fog-cloud situation and utilizing strategies for feature optimization.
Mohammad et al.[17]	2022	Healthcare data security and prediction are improved by ASCP-IoMT, a lightweight, secure communication system enabled by AI.	Replay, MITM, Ephemeral secret leakage (ESL)	SVM, DT, LR	By adding new functional capabilities like blockchain integration the protocol is improved.
Sahshanu et al.[18]	2022	New technologies to address issues in e-healthcare, such as PUF, Blockchain, AI, and SDN.	DDoS	Naive Bayes, RF	Improving the performance efficiency and accountability of AI applications in IoMT.
Panagiotis et al.[19]	2022	IDPS detect and reduce cyberattacks on industrial healthcare systems that target the IEC 60870-5-104 protocol by utilizing ML and SDN technologies.	DoS, Replay, MITM, Spoofing	SVM, RF, LR, DT, Naive Bayes	Improving the IDPS ability to identify multistep cyberattacks using ML-based association rules addresses that target IEC 60870-5-104 and other industrial and IoMT protocols in the healthcare industry.
Bandar et al.[20]	2023	A framework combining blockchain technology with machine/deep learning models is being developed to improve IoT device security by identifying and detecting cyberattacks.	DDoS, Spoofing, DoS	SVM, KNN, DT	Using the proposed structure on datasets from IoMT devices to find more trustworthy AI models and safeguard each IoT layer against certain assaults.
Fazlullah et al.[21]	2023	A fog-cloud architecture and ensemble learning-based cyberattack detection technique for IoMT networks.	Ransomware, DDoS	DT, RNN	A real fog-cloud scenario and using many feature selection techniques to optimize features.
Sotirios et al.[22]	2024	The application of AI methods, especially ML and DL to enhance IoMT device cybersecurity.	DoS, MITM, Sybil, Routing, DDoS	KNN-MLSC, SVM, AD	AI-powered solutions, particularly in the areas of data-driven healthcare and patient data protection.

Chapter 3

Challenges and Limitations

1. **Data Security** : The healthcare ecosystem is vulnerable to cyber assaults because of the volume of private patient data that is shared throughout networked devices. Cyberattacks, unauthorised access, and data breaches present serious dangers that might jeopardise patient privacy and the accuracy of medical data. To protect against these security risks, healthcare IoT systems need to use strict access restrictions, secure communication routes, and cutting-edge encryption technologies. A comprehensive plan that addresses data security concerns in the context of healthcare IoT and fosters a dependable and strong healthcare infrastructure also has to include regular upgrades, continuous monitoring, and adherence to industry standards.

2. **Interoperability** : The large range of manufacturers, devices, and communication protocols that prevent data interchange and integration from happening smoothly. Healthcare IoT devices often operate in silos, which complicates the process of several systems effectively integrating with one another. The lack of standard interfaces and protocols makes it difficult for critical patient data to be shared across devices and healthcare systems. This hinders the ability to assemble a comprehensive picture of a patient's medical data, which has an impact on the efficiency with which healthcare is provided. Interoperability problems need to be fixed in order to properly exploit IoT in healthcare. This necessitates the development and adoption of standardised procedures in addition to the collaboration of all parties involved in the healthcare system.

3. **Scalability** : The number of linked devices is rising, and healthcare systems are becoming more sophisticated. The infrastructure has to be able to handle this increase in data and device interactions as the number of IoT devices increases to improve general healthcare administration, diagnostics, and patient monitoring. System responsiveness and data processing delays may result from scalability problems, which can also show up as network congestion, data overload, and a pressure on computational resources. Healthcare IoT systems must be able to handle an ever-expanding network of devices and data without sacrificing patient care or performance. This can be achieved by addressing the scalability challenge with flexible communication protocols, effective data management techniques, and strong infrastructure design.

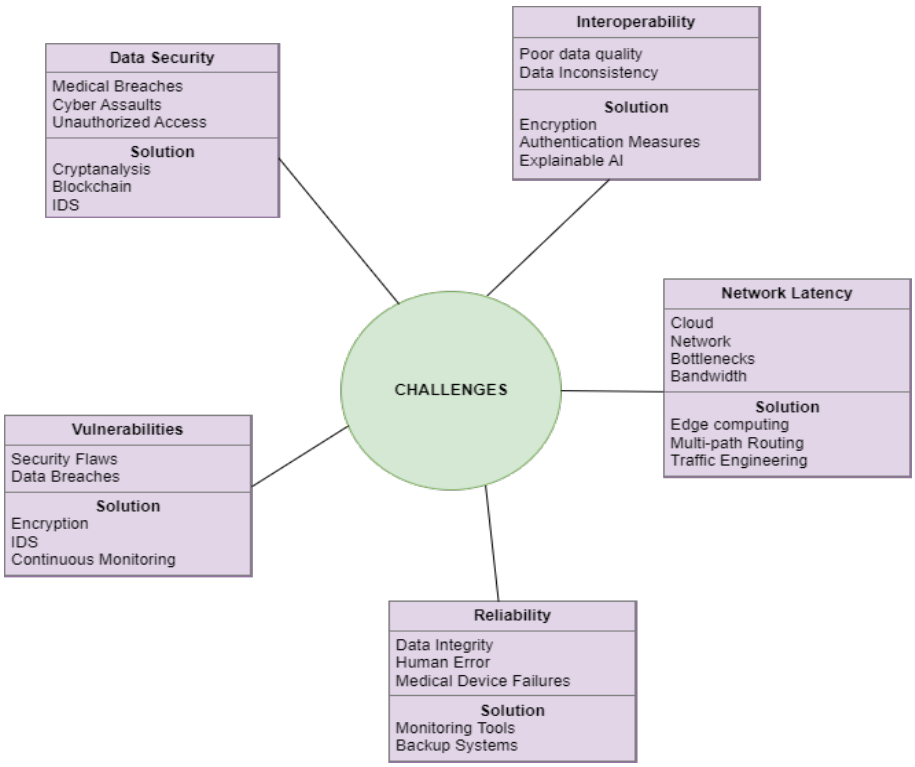

Figure 3.1: Challenges and Solution for IoT-Healthcare

4. **Reliability** : IoT systems and devices must function reliably and accurately in medical environments. Ensuring the accuracy of data gathered from different sources is essential for making well-informed decisions on healthcare. Healthcare IoT applications might be less successful due to problems like broken devices, poor connection, or inaccurate data. Resolving issues with system resilience, data correctness, and device robustness is necessary to get a high degree of reliability. Adopting

standardised methods, integrating redundant systems, and putting in place strict testing protocols are some ways to improve the overall dependability of healthcare IoT implementations. Resolving these issues is crucial to increasing IoT technology adoption in the healthcare industry and establishing consumer trust in them.

5. **Network Latency** : Affecting the vital medical data real-time delivery. Delays in data transmission can have major repercussions in the healthcare industry, particularly during surgical procedures or patient surveillance. When important information is sent to healthcare providers or when prompt actions are activated, network latency might cause delayed reaction times. When low-latency communication is essential to preserving the integrity of medical services, this problem is very apparent. Improved network speeds and responsiveness in healthcare IoT applications may be achieved by using technologies like 5G, implementing edge computing solutions to analyse data closer to the source, and optimising communication protocols.

6. **Vulnerabilities** : Due to the fact that several security risks might affect these networked devices. Medical equipment are a varied ecosystem with a lack of strong built-in security safeguards, which leaves them open to cyberattacks. Typical weaknesses encompass insufficient encryption, feeble authentication protocols, and antiquated software. Unauthorised access to private patient information, device tampering, or interruptions in medical services might result from an IoT security breach in the healthcare industry. Strict procedures including frequent software upgrades, encryption mechanisms, and all-encompassing cybersecurity frameworks must be put in place in order to ensure the security of healthcare IoT and protect patient data and medical device integrity.

7. **Cost** : Healthcare budgets may be strained by the costs of obtaining, implementing, and maintaining IoT devices, infrastructure, and security measures. The ongoing costs for data storage, analytics, and employee training add even more to the financial strain. Healthcare IoT has many potential benefits, including better patient outcomes and operational savings, but organisations need to carefully balance them against the costs. To overcome the financial barriers and guarantee the widespread and sustained implementation of IoT in healthcare, it is imperative to identify economical solutions, leverage economies of scale, and explore feasible business models.

8. **Standardization** : The lack of widely used frameworks and standards for data formats, security precautions, and device connectivity. Medical equipment come in a variety of forms, and their differing standards might cause problems with interoperability that impede smooth integration and data sharing. One of the main obstacles to guaranteeing the confidentiality and privacy of medical data sent across various devices is the absence of established protocols. The creation and acceptance of common protocols, data formats, and security standards within the healthcare IoT environment are necessary to address standardisation problems. The use of uniform frameworks is expected to foster interoperability, augment data security, and expedite the extensive integration of IoT technology inside healthcare environments.

Chapter 4

Proposed Approach

The quality of life of users has increased as a result of the incorporation of smart healthcare into daily activities. Wearable technology, IoT sensors, mobile devices, dynamic databases for information access and the Internet are just a few of its numerous components. They maintained a constant connection to exchange real-time heath data from wearable technology with various prediction services in an effort to enhance consumers health. Nevertheless, this method is susceptible to a number of security flaws including injection attacks, session hijacking, privilege escalation, distributed denial of service (DDoS) and easy manipulation of medical data by an attacker who wishes to mislead a healthcare professional. Consequently a safe architecture that is capable of analyzing the attackers malevolent behavior is required. This section introduces the working of the proposed architecture that is divided into four layers as shown in Figure 7,i.e., data acquisition, data analysis, blockchain layer and application layer. A comprehensive description of each layer is as follows.

4.1 Data Acquisition Layer

This layer consists of several IoT sensors that are positioned on the human body in the suggested design including immersive helmets, smart bands, hearing aids and brain interfaces. These sensors gather the body current state of health the EEG for instance registers any anomalies in the brain, smartwatches track blood pressure, heart rate and breathing rate and smart shoes offer a users posture, calories burned and step count. The smartphone has an implied application interface built into these wearable gadgets. The

information is kept in a centralized system usually one that nation-states purchase such a healthcare information system (HIS). This medical knowledge is essential for any medical professional, physician, drug expert and medical facility to forecast an unidentified illness and create a pandemic medication, population control and decision-making procedure. Healthcare data include social security numbers, radiographic pictures, insurance claims and diagnosis records among other important personal information about its users. Data manipulation and network assaults are two ways in which an attacker might get data for malicious reasons. As a result, AI-blockchain based architecture has been presented to analyse network attacks and classify the correct and attacked data.

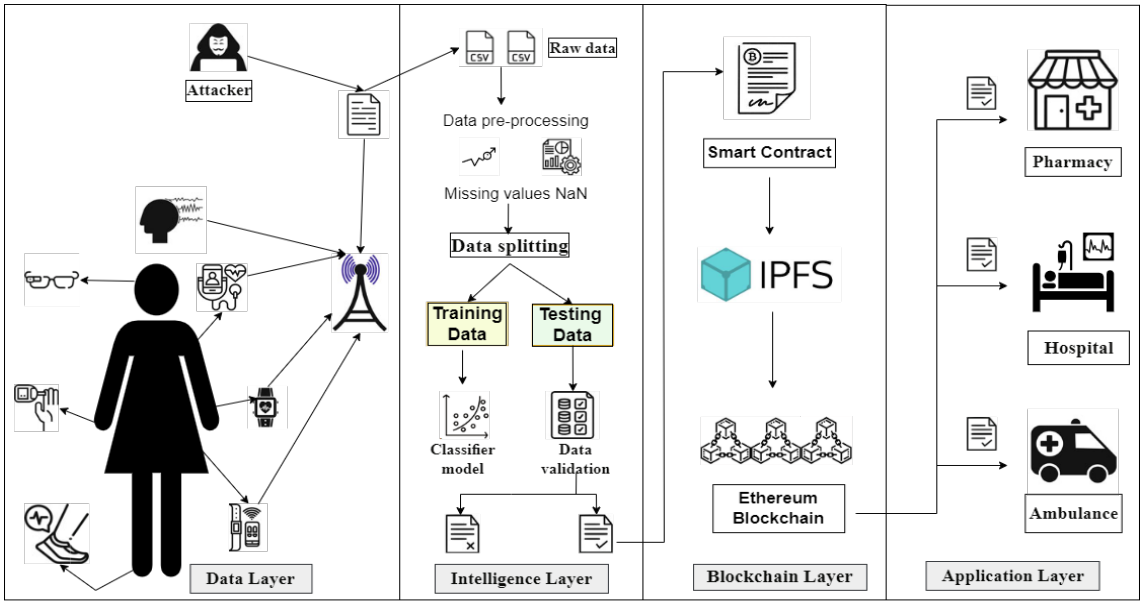

Figure 4.1: AI and Blockchain based smart and secure healthcare architecture.

4.2 Intelligence Layer

This layer combines machine learning classifiers to examine medical data for improper behaviour. In order to accomplish this an analysis log file kept by each wearable device must be obtained. A raw dataset may be created by looking through the log files important warnings and network activity. The gathered raw dataset is transformed into a comma-separated value (CSV) file, which is a format suitable with machine learning. Let D represent the total amount of raw data collected from various sources. The total data can be expressed as $D = \sum_{i=1}^{n} d_i$, where d_i is the data collected from the i-th source (e.g., wearable devices, medical records). The data D is split into training data D_{train}

and testing data D_{test}. Typically, the data is split into a ratio r.

$$D_{\text{train}} + D_{\text{test}} = D \tag{4.1}$$

$$D_{\text{train}} = r \cdot D \tag{4.2}$$

$$D_{\text{test}} = (1 - r) \cdot D \tag{4.3}$$

It contains attack data as well as healthcare data from any user who has wearable devices attached to their body. Attack data must be removed from normal data in order to prevent doctors from misguiding patients and endangering lives. On the other hand normal data help doctors diagnose patients more thoroughly. From the perspective of ML it is a binary classification problem that is normal data is classified as 0 and attack data is classified as 1. As the raw dataset contains outliers that might confuse the classifiers it must be preprocessed before being fed to the learning models in order to complete the classification job. Few numbers in the data columns will be huge and few will be little if the data is not normalized. The learning model may get biased if there are missing values in the columns. As a result the dataset undergoes preprocessing procedures that include feature selection, normalization, outlier identification and filling in missing values. Next the balanced dataset is divided into train and test data to validate the final prediction. The training data D_{train} is used to train a classifier model M. The accuracy A of the model is validated using the testing data D_{test}. The output is based on various performance metrics such as accuracy, precision, recall and F1 score value.

$$M = \text{Train}(D_{\text{train}}) \tag{4.4}$$

$$A = \frac{\text{Correct Predictions}}{\text{Total Predictions}} \tag{4.5}$$

4.3 Blockchain Layer

The Blockchain Layer uses decentralized ledger technology to ensure the data security, integrity and transparency. Health data is safely stored in this decentralized storage system. Data availability and tamper-proof records are guaranteed. A blockchain ledger is a secure, transparent and unchangeable record of exchanges of data that may only be viewed by authorized parties. The conditions of the agreement are directly encoded into

code in these self-executing contracts. They automate and uphold agreements between various parties, such those pertaining to data exchange between pharmacies and hospitals. By using consensus algorithms the blockchain prevents fraud and inconsistencies by guaranteeing that all participating nodes concur on the authenticity of transactions. Every organisation that uses this system including pharmacies, ambulance services and hospitals has a unique smart contract. By doing away with the need for middlemen and lowering the possibility of human mistake, these self-executing contracts automate and enforce agreements between different parties, such as those relating to data sharing between pharmacies and hospitals. By receiving data straight from entities these smart contracts expedite the procedure and guarantee data integrity. Predictive data improves accountability and transparency by being made publicly available on the blockchain upon submission to the smart contract and deployment. Additionally, depending on predetermined criteria this automation sets off automated warnings and actions that streamline operations cut down on administrative burden and improve the effectiveness of healthcare delivery like restocking medicine or arranging appointments. Let B be the data stored on the blockchain, including training results and predictions. The data B can be expressed as $B = f(D_{\text{train}}, M, D_{\text{test}})$, where f is a function representing the storage process involving encryption and consensus algorithms. Access to data on the blockchain is controlled and can be represented as Access B, where a_i represents access permissions for the i-th authorized entity (e.g., hospitals, pharmacies). Smart contracts S automate data exchanges and transactions, where g is a function representing the execution of the smart contract, and C are the conditions encoded in the contract.

$$AccessB = \sum_{i=1}^{m} a_i \tag{4.6}$$

$$S = g(B, C) \tag{4.7}$$

4.4 Application Layer

The application layer is where the insights and processed data are applied to practical healthcare applications improving the overall quality of treatment. This layer includes several use cases including pharmacies, hospitals, ambulances and other medical facilities where verified healthcare data is employed for expedited clinical trials, early diagnosis,

quick tracking and reporting of disorders and quick medication development. In a medical emergency this layer also handles prompt information exchange between the wearable device and medical professionals. When a patient experiences a heart attack while at a remote place for instance his wearable gadget tries to convey this information network to the hospitals in the area. By leveraging patient data to individually customise therapies to each patients needs this layer helps personalised medicine by increasing effectiveness and decreasing side effects. Applications for telemedicine use this data to offer remote consultations which are especially helpful in underserved or rural regions since they allow patients to get professional advice without having to travel there. This layer can also be used by healthcare practitioners to continuously monitor chronic illnesses enabling prompt modifications to treatment programmes based on real-time data from wearable devices. Pharmacies may expedite the prescription procedure by employing secure data to swiftly verify and administer medicine saving patients wait times. Furthermore, this layer helps emergency medical services (EMS) by providing prearrival information that helps them plan ahead and treat the patient more effectively when they arrive. Let U represent the utilization of processed data in practical applications such as emergency responses and clinical trials. The utilization U can be expressed as $U = h(B, S)$, where h is a function representing the application processes that use blockchain-stored data and smart contract outputs. In case of an emergency detected by a wearable device, the information $I = k(w)$ transmitted to medical professionals, where w represents the data from the wearable device, and k is the function handling the transmission and notification process. Combining these processes the overall system can be summarized as System Output = Apply(U, I). The application of real-time data and processed data to enhance healthcare results.

Chapter 5

Results and Discussions

The experimental setup and experimental analysis of the IoMT framework model architecture, which is based on the medical security database are covered in this part. The results are explained in below.

5.1 Experimental Setup

The proposed approach is implemented in stages. The first stage involves categorising the medical IoT data as normal or under attack. First, google colab is used to perform the classification. Several libraries are utilised here for data preprocessing, data balancing and classification, including Numpy (1.25.1), Matplotlib (3.7.2), imbalanced-learn, Sklearn and Pandas (2.0.3). In particular, Numpy is used for numerical operations and data manipulation while Pandas is used for dataset management and data cleaning. Matplotlib is used for data visualisation in computations. After the data has been categorised into

Table 5.1: Experimental Setup

Parameters	**Value**
Dataset name	WUSTL-EHMS-2020
Normal samples	14,272 (87.5%)
Attack samples	2,046 (12.5%)
Total number of samples	16,318
Libraries	Pandas, Numpy, Matplotlib, Sklearn
Language	Python programming language
Machine learning models	SVM, RF and K-NN

the normal (0) and attack (1) groups.

5.2 Results

The medical security dataset [23] was used in this study to apply SVM, RF and K-NN. This dataset has 16318 records from this year and it has attack can be attacked through any medical device. Here we can apply various machine learning algorithms and conclude its output given below :

In AI-based cybersecurity for medical IoT, normal behavior is defined as the typical, expected behavior of devices and networks in a medical environment. Attack behavior, on the other hand, refers to any malicious activity or unauthorized access that threatens the security of medical IoT devices and the confidentiality, integrity, and availability of the medical data they handle. AI-based cybersecurity solutions use machine learning algorithms to learn and distinguish between normal and attack behavior. For example, they can analyze network traffic patterns, device performance metrics, and system logs to identify anomalies that could indicate a potential attack. They can also monitor for known attack signatures and use threat intelligence data to quickly detect and respond to emerging threats.

The next evaluation criterion is the confusion matrix (CM). The performance of ML approaches is measured by the generation of CM. The results of SVM, RF, and K-NN classification using CM are shown in Fig. 4, 5 and 6. In the CM, column indicate the predicted labels, while rows represent true labels. For SVM, the True Positive (TP) and True Negative (TN) samples are represented by the main diagonal, which is 192 and 425, respectively. Likewise, the values of False Negatives (FN) and False Positives (FP) are 192 and 10, respectively. For RF, the values of TP are 190, TN are 430, FP are 5, and FN are 194. However, K-NN has TP of 342, TN of 349, FP of 86, and FN of 42. Therefore, we conclude from CM results that K Nearest Neighbor outperforms other ML approaches in terms of classification results.

The total performance of each classification approach is determined using the TP, TN, FP, and FN in terms of accuracy (AC), precision (PR), recall, and F1 score. The

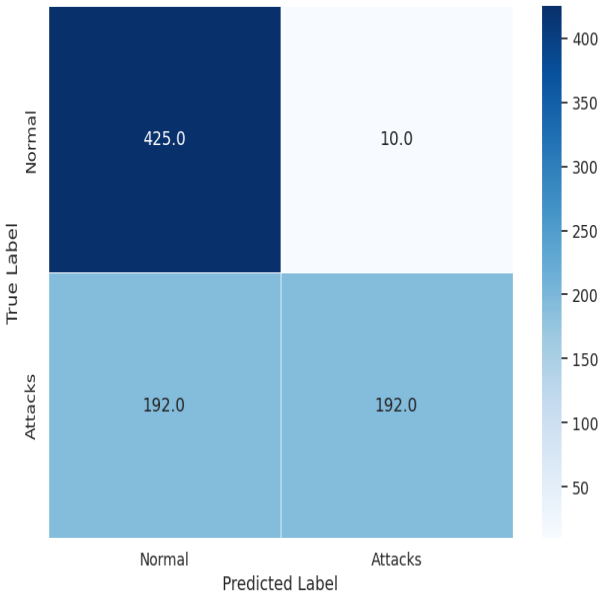

Figure 5.1: Confusion matrix for SVM

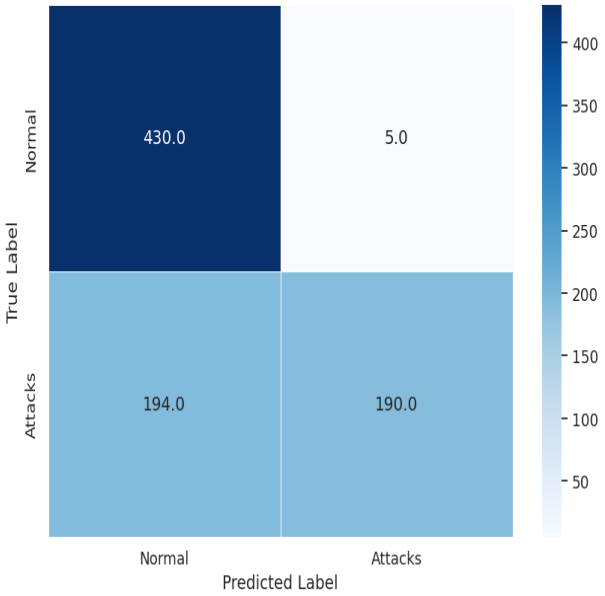

Figure 5.2: Confusion matrix for RF

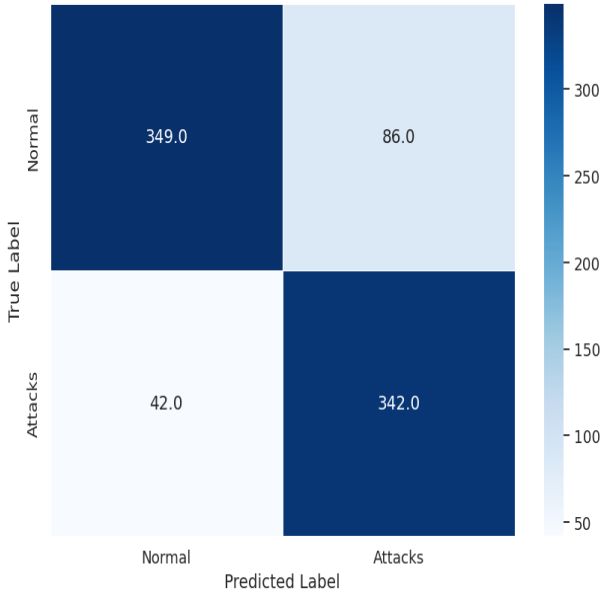

Figure 5.3: Confusion matrix for K-NN

performance results of the detection system utilizing each classification method are displayed in Fig. 8, 9, 10 and 11. Additionally, the detection model using SVM obtained AC of 75.33%, PR of 81%, recall of 75%, and F1 score of 74%. Regarding RF, the total performance is 75.94% for AC, 83% for PR, 76% for recall, and 74% for F1 score. In the same way, AC is 84.39%, PR is 85%, recall is 84%, and F1 score is 84% for K-NN. Therefore, we can say that in terms of AC, PR, recall, and F1 score, the K-NN has done better.

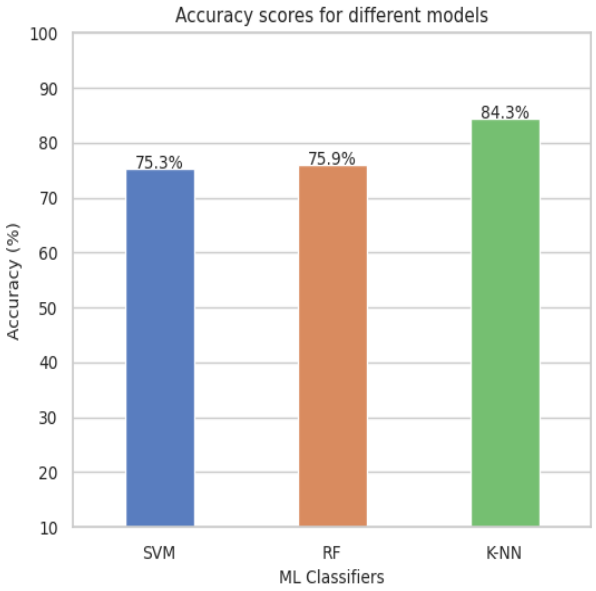

Figure 5.4: Performance comparison in terms of accuracy

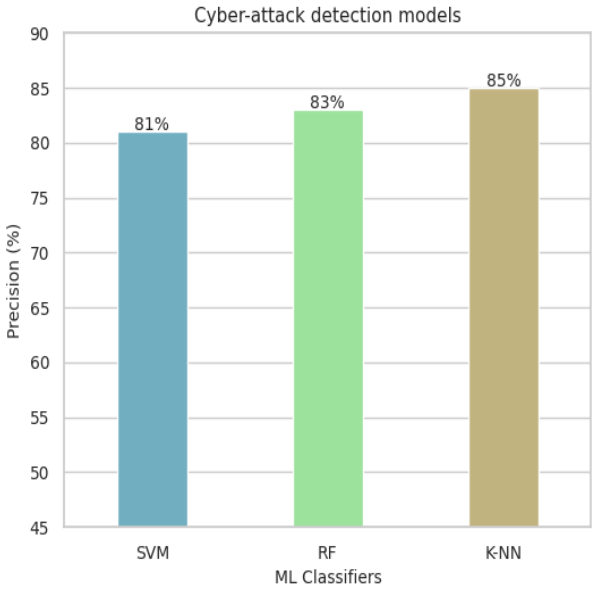

Figure 5.5: Performance comparison in terms of precision

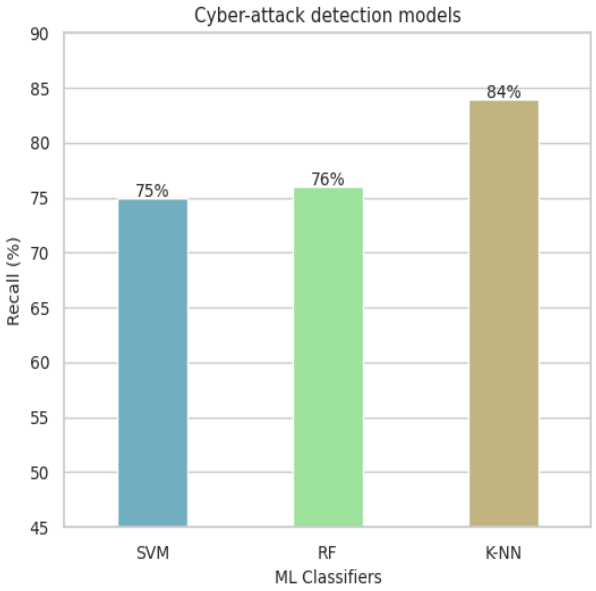

Figure 5.6: Performance comparison in terms of recall

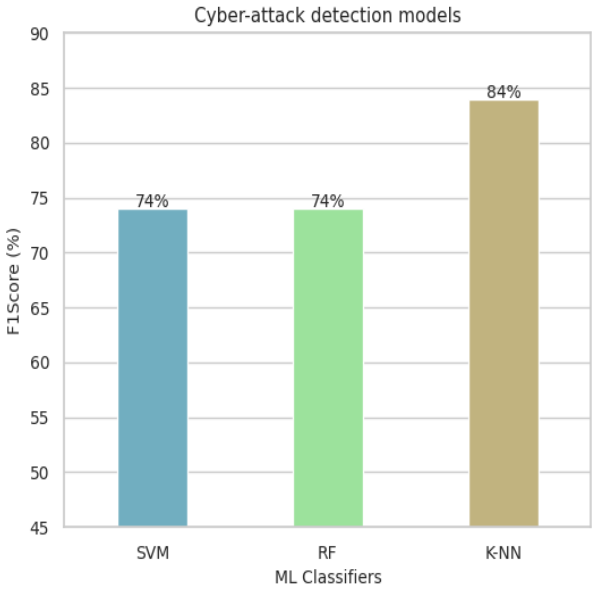

Figure 5.7: Performance comparison in terms of F1Score

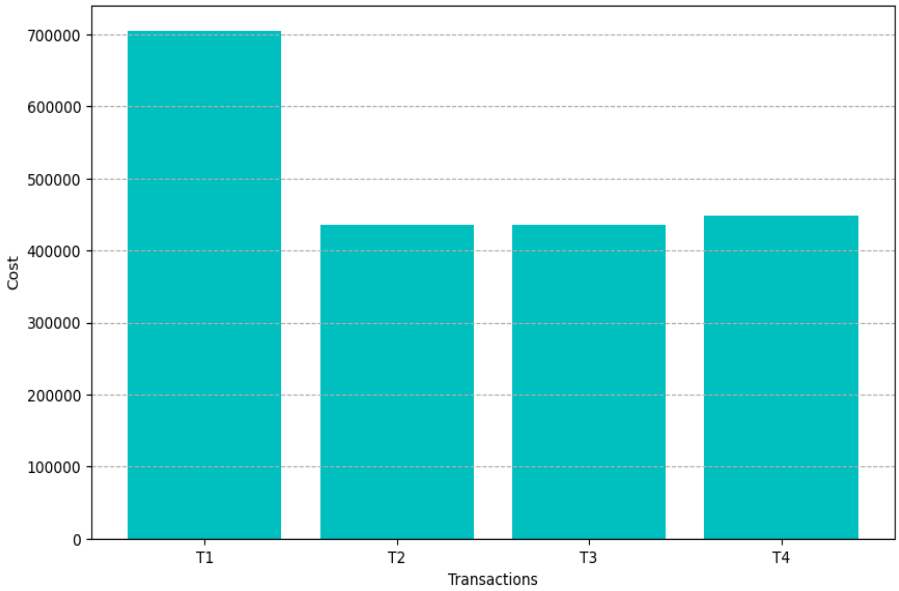

Figure 5.8: Transaction Cost

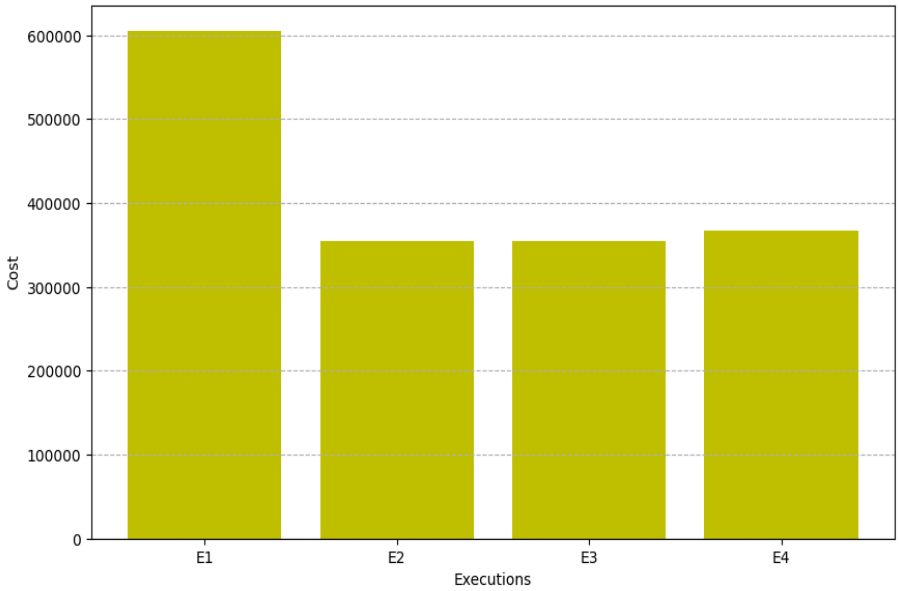

Figure 5.9: Execution Cost

Chapter 6

Conclusion and Future Scope

Our study highlights IoT improves patient care and treatment by using the capabilities of sensors, data analytics, and connected devices. In this work, different ML classifiers, such as SVM, RF, and KNN, are used to classify healthcare data into attack and normal classifications. Additionally, a variety of performance evaluation criteria have been taken consideration, such as F1 score, accuracy, precision, and recall. When compared to other ML classifiers, KNN gets the greatest accuracy in this case, at 84.3%. In future directions using explainable AI in our next case study to improve our strategy. In order to determine which elements are most important for our AI models to take into consideration. Explainable AI will examine the features in our dataset and offer insights. Focusing on the most significant elements this instruction might increase model accuracy. we will explore methods like LIME, SHAP and ELi5 for explainability. On the other side, we will create a decentralized application using the blockchain technology to ensure security and transparency in data handling and transactions.

Bibliography

[1] R. Arul, Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib, and M. J. Piran, "Multi-modal secure healthcare data dissemination framework using blockchain in iomt," Personal and Ubiquitous Computing, pp. 1– 13, 2021.

[2] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems secu- rity," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707–8718, 2020.

[3] T. Krishna, S. P. Praveen, S. Ahmed, and P. N. Srinivasu, "Software- driven secure framework for mobile healthcare applications in iomt," Intelligent Decision Technologies, vol. 17, no. 2, pp. 377–393, 2023.

[4] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne, "A survey of wearable devices and challenges," IEEE Communications Surveys Tutorials, vol. 19, no. 4, pp. 2573–2620, 2017.

[5] A. Rana, C. Chakraborty, S. Sharma, S. Dhawan, S. K. Pani, and I. Ashraf, "Internet of medical things-based secure and energy-efficient framework for health care," Big Data, vol. 10, no. 1, pp. 18–33, 2022.

[6] B. Panchal, S. Parmar, T. Rathod, N. K. Jadav, R. Gupta, and S. Tanwar, "Ai and blockchain-based secure message exchange framework for med- ical internet of things," in 2023 International Conference on Network, Multimedia and Information Technology (NMITCON). IEEE, 2023, pp. 1–6.

[7] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and arti- ficial intelligence in internet of medical things: architecture, technology and application," IEEE access, vol. 8, pp. 101 079–101 092, 2020.

[8] J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, J. Garg, and G. J. Ajamu, "Aiiomt: Iomt-based system-enabled artificial intelligence for enhanced smart healthcare systems," Machine learning for critical Internet of Medical Things: applications and use cases, pp. 229–254, 2022.

[9] "Iomt architecture overview," https://inxee.com/blog/ iomt-architecture-overview/, accessed: 2024-03-22.

[10] "Application of artificial intelligence in wearable devices: Opportunities and challenges," Computer Methods and Programs in Biomedicine, vol. 213, p. 106541, 2022.

[11] M. Usman, M. A. Jan, X. He, and J. Chen, "P2dca: A privacy- preserving-based data collection and analysis framework for iomt appli- cations," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1222–1230, 2019.

[12] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "Sdn orchestration to combat evolving cyber threats in internet of medical things (iomt)," Computer Communications, vol. 160, pp. 697– 705, 2020.

[13] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," Computer Communications, vol. 166, pp. 110–124, 2021.

[14] S. Khan and A. Akhunzada, "A hybrid dl-driven intelligent sdn-enabled malware detection framework for internet of medical things (iomt)," Computer Communications, vol. 170, pp. 209–216, 2021.

[15] K. Haseeb, I. Ahmad, I. Awan, J. Lloret, and I. Bosch, "A machine learning sdn-enabled big data model for iomt systems. electronics 2021, 10, 2228," 2021.

[16] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application," IEEE Access, vol. 8, pp. 101 079–101 092, 2021.

[17] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. P. C. Rodrigues, "Ascp-iomt: Ai-enabled lightweight secure communication protocol for internet of medical things," IEEE Access, vol. 10, pp. 57 990–58 004, 2022.

[18] S. Razdan and S. Sharma, "Internet of medical things (iomt): Overview, emerging technologies, and case studies," IETE technical review, vol. 39, no. 4, pp. 775–788, 2022.

[19] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach," IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2041–2052, 2021.

[20] B. M. Alshammari, "Aibpsf-iomt: Artificial intelligence and blockchain- based predictive security framework for iomt technologies," Electronics, vol. 12, no. 23, p. 4806, 2023.

[21] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. ur Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in iomt," IEEE Transactions on Industrial Informatics, 2023.

[22] S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras, and N. Doulamis, "Enhancing internet of medical things security with artificial intelligence: A comprehensive review," Computers in Biology and Medicine, p. 108036, 2024.

[23] Unal, D., et al. "WUSTL EHMS 2020 dataset for internet of medical things (IoMT) cybersecurity research (2019)." (2021).