Palestine Polytechnic University

Deanship of Graduate Studies and Scientific Research

Master of Informatics

Enhancing IoMT Security using Multi-Layer Authentication: ZTM and ML-Based Case Study

Submitted by:

Basma Mohammad Abu Sabha

Supervised by:

Dr. Radwan Tahboub

Thesis submitted in partial fulfillment of requirements of the degree

Master of Science in Informatics

November, 2025

The undersigned hereby certify that they have read, examined, and recommended to the Deanship of Graduate Studies and Scientific Research at Palestine Polytechnic University the approval of a thesis entitled "Enhancing IoMT Security using Multi-Layer Authentication: ZTM and ML-Based Case Study" submitted by Basma Mohammad Abu Sabha in partial fulfillment of the requirements for the degree of Master in Informatics.

Graduate Advisory Committee:

Dr. Radwan Tahboub (Supervisor), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr. Mousa Farajallah (Internal committee member), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr.Mohannad Al-jabari (External committee member), Hebron University.

Signature:_____ Date:_____

Thesis Approved

Prof. Mahmoud AlHaddad

Dean of Graduate Studies and Scientific Research

Palestine Polytechnic University

Signature: _____ Date: _____

DECLARATION

I declare that the Master Thesis entitled **'Enhancing IoMT Security using Multi-Layer Authentication: ZTM and ML-Based Case Study'** is my original work and hereby certify that unless stated, all work contained within this thesis is my independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Basma M. Abu Sabha

Signature: _____ Date: _____

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for the master degree in Informatics at Palestine Polytechnic University, I agree that the library shall make it available to borrowers under rules of the library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made. Permission for extensive quotation from, reproduction, or publication of this thesis may be granted by my main supervisor, or in his absence, by the Dean of Graduate Studies and Scientific Research when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Basma M. Abu Sabha

Signature: _____ Date: _____

الملخص

مع تزايد استخدام أجهزة الإنترنت الطبية في سيارات الإسعاف، أصبح بالإمكان نقل العلامات الحيوية للمرضى بشكل فوري إلى المستشفيات. إلا أن هذا التبادل أصبح معرضًا للتهديدات السيبرانية، خصوصًا هجمات رفض الخدمة وهجمات حقن البيانات أو الانتحال، والتي قد تؤخر اتخاذ القرارات الحرجة وتهدد سلامة المرضى. تخضع أنظمة الإنترنت الطبية لعدة أنواع من الهجمات عبر طبقات مختلفة. بينما تركز الحلول الحالية على تأمين البيانات الطبية من خلال التشفير أو البلوك تشين في البيئات الطبية المتنقلة، فإنها لا تركز على اكتشاف الشذوذ أثناء النقل أو تحليل سلوك الشبكة ومحتوى البيانات في الوقت الفعلي.

تقترح هذه الأطروحة إطارًا أمنيًا يعمل في الوقت الفعلي لخدمات الطوارئ الطبية، يقوم بالمراقبة والتحليل المستمر على مستويين: الشبكة ومحتوى البيانات، استنادًا إلى مبدأ «لا تثق أبدًا، تحقق دائمًا». يهدف هذا الإطار إلى اكتشاف التهديدات واتخاذ إجراءات فورية قبل وصول البيانات إلى المستشفى.

يدمج النموذج تقنيات التعلم الآلي، ونظام كشف التسلل المبسط، ونموذج الثقة الصفرية، والمصادقة الثنائية لمحاكاة التطبيق على مستويين: (١) هجمات رفض الخدمة على مستوى الشبكة مع وصف عام ومحاكاة محدودة؛ (٢) هجمات حقن البيانات على مستوى المحتوى مع تركيز ومناقشة تفصيلية على هذا المستوى. عند اكتشاف هجوم، يطبق النظام آلية عزل تقوم بعزل الجهاز المخترق من شبكته داخل سيارة الإسعاف في حالة هجوم حقن البيانات، أو فصل واجهة شبكة سيارة الإسعاف في حالة هجوم رفض الخدمة على مستوى الشبكة، مما يمنع انتشار الحركة الخبيثة. يتم تدريب مصنفات التعلم الآلي مثل شجرة القرار، والجيران الأقرب، والغابات العشوائية في السحابة (المستشفى في نموذجنا)، ثم تُختبر عند العقدة الطرفية (سيارة الإسعاف)، لضمان اتخاذ قرارات في الوقت الفعلي وتحسين استهلاك الموارد ضمن بيئات طبية متنقلة.

أظهرت نتائج المحاكاة أن نموذج شجرة القرار حقق أفضل أداء في التصنيف متعدد الفئات على مستوى محتوى البيانات (هجوم، مشكلة طبية، طبيعي)، بدقة كلية بلغت ٩٨,٠٩٦٪ ومعامل ارتباط ماثيوز بقيمة ٩٧,١٧٢٪، مقارنة بالنماذج الأخرى، بما في ذلك الغابات العشوائية بدقة ٩٨,٠١٪ ومعامل ارتباط ٩٧,٠٥٥٪، والجيران الأقرب بدقة ٩٧,٧٢٪ ومعامل ارتباط ٩٦,٥٦٪.

الكلمات المفتاحية - لغة الآلة، انترنت الأجهزة الطبية، خدمات الطوارئ الطبية، نموذج الثقة الصفرية، المصادقة الثنائية.

Abstract

The growing use of the Internet of Medical Things (IoMT) in ambulances enables real-time transmission of patients' vital signs to hospitals. However, this exchange is increasingly exposed to cyber threats, especially Distributed Denial of Service (DDoS) and data injection or spoofed attacks that can delay critical decisions and compromise patient safety. This IoMT system is subject to various kinds of attacks across multiple layers. While many existing solutions focus on securing medical data through encryption or blockchain in a mobile medical environment, they do not focus on detecting anomalies during transmission or analyzing network and data content behavior in real-time. This thesis proposes a real-time security framework for Emergency Medical Services (EMS) that continuously monitors and analyzes both levels, network and data content, based on the principle of "never trust, always verify." The aim is to detect specific threats and take immediate action in real time before the data reach the hospital. The model integrates Machine Learning (ML), a Signature Intrusion Detection System (SIDS), the Zero Trust Model (ZTM), and Two-Factor Authentication (2FA) to simulate the application at two levels: (1) DDoS attacks at the network level with a general description and less simulation; (2) data injection attacks at the content level with focusing and discussion in detail at this

level. Once an attack is detected, the system applies an isolation mechanism that either isolates the compromised IoMT device from its network at the ambulance in case data injection comes from that device, or disconnects the ambulance's network interface in case of DDoS at the network level, preventing further propagation of malicious traffic. ML classifiers such as Decision Tree (DT), K-Nearest Neighbors (KNN), and Random Forest (RF) are trained in the cloud represented in our work by the hospital and then tested at the edge node (ambulance), which is the closest point to the data collection to ensure real-time decision-making and optimize resource usage under the constraints of mobile medical environments. The simulation results demonstrate that the DT model achieved the best performance for multiclass classification at the data-content level (attack, medical issue, normal), with an overall accuracy of 98.096% and an Matthews' Correlation Coefficient (MCC) of 97.172%. This compared with other models, including RF with an accuracy of 98.01% and MCC of 97.055%, and KNN with an accuracy of 97.72% and MCC of 96.56%.

Keywords: IoMT, ZTM, 2FA, EMS, ML.

DEDICATION

To my ambitious self, who endured every challenge and never gave up until this work was complete, to my patient and supportive supervisor whose guidance lit my path,to my beloved mother, the endless source of my compassion and strength; to my dear father, the source of my support and guidance; to my loving husband Mohammad and my precious children Omar and Celena; to my brothers and sisters, pieces of my soul; to my wonderful friends Danya, Raeda, Tala, and Sabha; and to everyone whose support, in both small and great ways, contributed to the successful completion of this work.

Basma M. Abu Sabha

Acknowledgements

First, I would like to thank Allah for giving me the strength and patience to complete this work. I would like to express my sincere gratitude to my supervisor, Dr. Radwan Tahboub, for his ongoing support and valuable guidance. I would also like to thank Dr. Hani Salah, Dr. Mousa Farajallah and Dr. Mohannad Al-jabari for their helpful feedback and suggestions. My deepest appreciation goes to my parents, husband, children, family, and friends, whose love, patience, and encouragement were the true source of strength throughout this journey.

Basma M. Abu Sabha

Contents

List of Figures

List of Tables

List of Algorithms

Acronyms

2FA Two-Factor Authentication

6LoWPAN IPv6 over Low-Power Wireless Personal Area Networks

AI Artificial Intelligence

AUC Area Under the Curve

DBP Diastolic Blood Pressure

D2D Device-to-device

D2E Device-to-Edge

DDoS Distributed Denial of Service

DT Decision Tree

E2C Edge-to-Cloud

ECC-AES Elliptic Curve Cryptography-Advanced Encryption Standard

ECG Electrocardiogram

ECDH Elliptic Curve Diffie-Hellman

EMS Emergency Medical Services

FNR False Negatives Rate

FPR False Positives Rate

HMAC Hash-based Message Authentication Code

HR Heart Rate

IBAC Identity-Based Access Control

IDS Intrusion Detection System

IoMT Internet of Medical Things

IoMV Internet of Medical Vehicles

IoT Internet of Things

IoV Internet of Vehicles

KNN K-Nearest Neighbors

LR Logistic Regression

MCC Matthews' Correlation Coefficient

MDA Mean Decrease in Accuracy

MDI Mean Decrease in Impurity

MFA Multi-Factor Authentication

MitM Man-in-the-Middle

ML Machine Learning

MQTT Message Queuing Telemetry Transport

NB-IoT Narrowband Internet of Things

NR New Radio

OOB Out-of-Bag

PIN Personal Identification Number

RF Random Forest

RR Respiratory Rate

SBP Systolic Blood Pressure

SFA Single-Factor Authentication

SIDS Signature Intrusion Detection System

SpO2 Oxygen Saturation

TLS Transport Layer Security

TLTO Trust and Latency-aware Task Offloading

ZTM Zero Trust Model

Chapter 1

Introduction

Internet of Things (IoT) represents the latest phase in the evolution of communications technology. It enables physical objects to be linked and empowered as sensors, which allows them to generate, access, and effectively share information. IoT has already been implemented in various fields, such as smart cities, smart environments, smart transportation, and emergency systems [1],[2].

IoMT is a growing part of IoT, where devices, sensors, and software are combined to enable the acquisition and sharing of medical data. IoMT is capable of revolutionizing healthcare with the advanced and therapeutic measures for a wide range of health conditions. It also ensures better engagement of patients in their healthcare, such as remote patient monitoring and emergency responses, offering significant improvements in care delivery and outcomes, and improving the quality of life of individuals and communities [3]. In healthcare systems, medical environments can

be classified as either static, such as hospitals, or mobile, such as Internet of Medical Vehicles (IoMV), which typically refers to connected ambulances equipped with IoMT devices, medical tools, and real-time communication capabilities. However, the increasing use of IoMT devices, such as pulse oximeters and smart thermometers, in healthcare systems is inviting the rise of cyberattacks. These ambulances play a dual role: technologically, they monitor and transmit patients' vital signs to hospitals in real time; medically, paramedics provide urgent care. Recent literature on EMS further emphasizes the role of the ambulance as a vital mobile unit within the pre-hospital emergency care chain [4, 5, 6, 7].

In this thesis, the term "ambulance" will refer specifically to a smart and connected medical vehicle which equipped with IoMT devices, and able to monitor and report patient vital signs in real-time. The term EMS will be used to denote the broader emergency care system that includes ambulances, medical personnel, IoMT devices, and communication infrastructure involved in pre-hospital care. Most IoMT devices are small, power-restricted, and easily available and are therefore vulnerable to cyberattacks. These limitations, like low computations and unreliable communications, are exacerbated in mobile healthcare environments such as ambulances. Due to their mobility and utilization of insecure communication protocols, IoMV systems generally face enhanced cybersecurity threats when sending patient data like vital signs in real-time. Additionally, the absence of standardized security protocols for medical devices exposed them to attack at various points in the network [4],[8]. IoMT changed the healthcare sector by creating medical devices and networked systems

that confidently collect, transmit, and store patient information. This technology facilitates healthcare professionals real-time knowledge, and workflow simplification, which in the end leads to an increase in the quality and efficiency of patient care. In the EMS system, the ambulance is being integrated with an advanced system consisting of IoMT monitoring a patient's heart rate and blood pressure, which constantly monitors the patient's vital signs. All data is continuously transmitted to the hospital database for immediate evaluation by the doctor in advance before the arrival of the patient [9].

Despite the critical role that smart ambulances have in the EMS system, the secure transmission of vital signs remains a challenge. Attacks targeting the network or IoMT devices or the medical data itself may lead to data loss, delays, or manipulation, potentially endangering patients' lives. Although scaling IoMT devices enhances healthcare monitoring and diagnosis, it also increases security vulnerabilities and makes them attractive targets for cyberattacks such as malware and DDoS, which threaten patient data and device functionality. [10],[11].

Few studies work on this area, and the existing solutions don't focus on providing real-time, dual-level protection at both the data content level (vital signs) and network traffic, which this study aims to address through a dual-layer approach, particularly suited for resource-constrained mobile environments. Due to the limitations in IoMT devices (low processing power and memory) the local computation is poor. This problem is solved by edge computing by making available neighboring com-

putational resources for real-time analysis. In enabling intelligent decision-making using AI. On the other hand, cloud dependence leads to latency and breaches in privacy, especially with health data that is sensitive [12],[13]. Therefore, the model is trained on the cloud using enormous volumes of data and deployed at the edge node, like a gateway or smart device in the ambulance, to perform light-weight, real-time anomaly detection on network traffic and patient data at the point of care.

This thesis aims to develop a security framework to protect patient data transmitted from IoMT devices during ambulance transport to the hospital by an integrated model that utilizes ML, SIDS, 2FA, and ZTM. It achieves this by analyzing both data content behavior and network traffic at the edge node located within the ambulance using ML techniques. Based on where the anomaly is detected originating from, the system can either isolate the infected medical device or the external network interface to quarantine the attack and preserve system integrity.

1.1 Problem Statement and Analysis

In EMS ambulances equipped with IoMT devices, vital signs of patients are transmitted to hospitals in real time to enable faster clinical decision making. However, this mobile transmission process is highly vulnerable to cyberattacks, particularly due to the constrained nature of mobile environments and the lack of standardized, secure communication protocols. Transmissions are subject to various kinds of attacks, such as DDoS and data injection attacks, that compromise patient safety even before patients have access to the hospital. A recent report by CyberPeace highlights

how DDoS attacks targeting healthcare systems have led to interrupted basic care services, delayed emergency response, and loss of life [14].

Although most existing studies have focused on securing data transmitted within hospital-based systems like encryption or blockchain technologies, limited research has addressed the security of EMS, particularly the communication between ambulances and hospitals. Most current studies focus on post-transmission protection, assuming that the connection and data transmitted from IoMT devices is already trustworthy. However, according to the ZTM principle, "never trust, always verify" this approach highlights the need for continuous verification of data during transmission through the network. Besides, common safety and cybersecurity standards such as ISO 26262 and ISO 14971 were designed for in-hospital or static environments and do not accommodate the unique challenges posed by mobile IoMT systems within ambulances [4]. Further, emergency medical personnel often operate without formalized risk management protocols to direct handling these compromised devices in transit. All of these gaps highlight the need for real-time, customized security practices dedicated to the EMS communications environment.

1.2 Motivation

The growing reliance on IoMT-enabled ambulances for real-time patient monitoring presents an urgent need for enhanced security mechanisms that go beyond traditional data protection techniques. Existing solutions largely focus on securing data at rest or in transit using blockchain or encryption, but they don't focus on evaluating the trustworthiness of the data source or detecting anomalies during live transmission.

Traditional security methods cannot effectively stop zero-day attacks and need a lot of computing power, which small IoMT devices with limited batteries cannot provide. EMS systems are vulnerable to attacks that could inject false medical data or disrupt communication entirely events that may lead to misdiagnoses, treatment delays, or even patient harm. Advanced machine learning techniques can help by learning from the large amounts of data generated by these devices to find new types of attacks more quickly and efficiently.

Motivated by these limitations, this thesis introduces a real-time integrated framework specifically designed for mobile EMS environments. The proposed approach tackles security threats on two fronts: at the network level, it detects DDoS attacks that aim to block the communication channel between the ambulance and the hospital; at the data level, it identifies injection attacks from compromised IoMT devices. By continuously analyzing both network and data content behavior, the system is able to detect anomalies early and apply an isolation mechanism that either isolates the compromised device from their network or disconnects the ambulance's network interface to minimizing further damage.

This thesis is particularly motivated by the lack of real-time practical solutions in the literature that address the mobile and vulnerable nature of ambulance environments. Through the integration of ML models, ZTM, SIDS, and 2FA with real-time response measures at the edge (ambulance), the proposed framework intriduce a significant improvement in protecting the flow of critical patient vital signs data before arrival at the hospital.

1.3 Research Objectives

This research aims to propose a security framework and attack detection in real-time by integrating ZTM, SIDS, ML, and 2FA in a mobile healthcare environment.
This research aims to address the following objectives:

1. Develop a real-time security framework for protecting patient vital signs transmitted from ambulances to hospitals.

2. To provide dual-level threat detection by detection of network-level attacks, such as DDoS. Data-level attacks, including spoofed or injected vital signs.

3. To enable real-time response actions at the edge (ambulance), such as isolating a compromised IoMT device or network interface for the ambulance temporarily until the issue is resolved by the security team, after notifying them about the problem.

4. Reduce latency and dependency on cloud infrastructure by deploying AI-based detection at the edge.

5. Balance security and performance, especially in mobile medical environments with limited computational resources, by using ML models.

1.4 Contributions

To the best of our knowledge, this is one of the first frameworks to integrate ML, SIDS, ZTM, and 2FA within a smart ambulance (IoMV) environment.
The main contributions of this study are as follows:

1. Proposed a good integrated security framework for a mobile healthcare system combining ZTM, SIDS, ML, and 2FA.

2. Introduced a dual-behavior analysis approach that monitors both network traffic and data content (vital signs) behavior.

3. Implemented an isolation mechanism at the edge (ambulance) that reacts to the type of threat:

   - Isolates a specific IoMT device if data is compromised.
   - Isolates the ambulance network interface if a DDoS is detected.

   Note: The isolation temporarily until the issue is resolved by the security team, after notifying them about the problem.

4. Integrated 2FA at the edge, ensuring that paramedics are not trusted by default, even by authorized personnel, unless verified.

5. Enabled intelligent differentiation between medical issues, cyberattacks, and normal cases, using ML-based classification to avoid medical misdiagnosis.

6. The system was simulated to operate in real-time on edge-level devices, showing that it could be effectively used in EMS.

7. Integrate ML model's result classification with ZTM at the data content level to determine the next suitable action, which reduces the False Positives Rate (FPR).

8. A comparison table of previous studies across multiple levels has been prepared, as illustrated in Chapter 3.

9. We simulated a synthetic attack dataset as a simplified case scenario consisting of approximately 81,000 records, and about 1,500 medical issue cases, and included the resulting dataset in the appendix for reuse.

1.5 Research Methodology

1. Developed a simulated framework integrating ML, SIDS, ZTM, and 2FA to secure IoMT data transmission.

2. Used two distinct datasets:

   - Network-level: ICU Healthcare Security Dataset, focusing on DDoS attacks.
   - Data-level: Human Vital Signs Dataset, used to simulate real and tampered vital signs.

3. Trained ML models in the cloud and tested them at the edge to ensure fast and efficient real-time anomaly detection.

4. Applied different ML algorithms such as DT, RF, KNN, and NB, suitable for low-resource devices in ambulances.

5. Simulated attacks by generating medically implausible data (e.g., unrealistic temperature or heart rate) that violated physiological logic and consistency with other vital sign readings, to test data integrity.

6. Implemented ZTM logic to isolate either the infected IoMT device or the ambulance's network interface, based on the source of the anomaly.

7. Used SIDS to analyze abnormal vital signs, determining if the issue is health-related or an injected cyberattack.

8. Evaluated system performance using standard metrics macro average for: Accuracy, Precision, Recall, and F1-Score. FPR, False Negatives Rate (FNR) for each class, Detection Time, Memory Usage, MCC, Cohen's kappa and Area Under the Curve (AUC).

1.6 Publications

- The following paper has been published at the IEEE CiSt'25 conference: B. Abu Sabha and R. Tahboub."Framework to Integrating IDS, Machine Learning, ZTM, and Two-Factor Authentication into IoMT Systems" in [AIMP'25] - 7th IEEE conference on Artificial Intelligence and Multimedia Processing (CiSt'25), presented on October 4, 2025, and the work has also been selected for publication in the open-access International Journal of Information Science and Technology (iJIST).

- Also the paper has been submitted and accepted for participation in the Scientific Research Award organized by the Ministry of Education, Palestine, 2025 – 3rd cycle "Research Priorities".

1.7 Thesis Organization

The rest of the document is organized as follows: Chapter 2 presents an introduction and background on IoMT system layers, as well as the key tools used in this work, including ZTM, SIDS, 2FA, and ML. It also presents an overview of the attack model addressed in this work. Chapter 3 presents a literature overview, and Chapter 4 presents the proposed system model and architecture. Implementation, simulation, and results are provided in Chapter 5. Finally, conclusions and future works are summarized in Chapter 6.

Chapter 2

Background

In recent times, healthcare and modern technology have received significant attention due to their growing impact on daily life and medical services. IoMT is a subsection of the broad area of IoT, mainly oriented at applications in the medical and healthcare fields. However, as the use of IoMT devices in healthcare keeps increasing, their security has become a major concern [15],[16].

2.1 IoMT in Palestine

Current research [59] shows a possible real-world implementation of IoMT solutions in Palestine, specifically in regards to the area of telemedicine for elderly individuals. In this regard, they designed a smart health monitoring system utilizing wearable sensors to detect vital signs such as pulse rate, oxygen level in the blood, body temperature, and Electrocardiogram (ECG), with real-time wireless data transmission to centrally hosted platforms for analysis and medical follow-up. This system was implemented to specifically counter the challenges experienced in Palestine in

terms of limited movement, poor health delivery infrastructure, and lack of medical professionals by allowing continuous health monitoring and subsequent medical interventions.

On a related note, other research conducted in Palestine suggests that health delivery frameworks designed under both IoT and IoMT have been successful in improving access to healthcare in underserved and distant regions by reducing the need for non-essential hospitalizations and improving health delivery decisions with real-time data availability [6].

2.2 IoMT Systems Architecture

Studies show that IoMT applications use various architectures based on their specific requirements and purposes. While each technology claims to be the best solution for a given application, they generally follow a three-layer structure, as shown in Figure 2.1.

Figure 2.1: The layers in IoMT architecture [17].

- Perception Layer: The foundational layer reads and collects health data using sensors and IoMT devices such as pacemakers, smartwatches, and oximeters. These devices transmit raw data to the network layer without processing [15].

- Network Layer: Is responsible for transmitting medical data from the gateway (edge node) to the cloud using various communication protocols such as Wi-Fi 6, Narrowband Internet of Things (NB-IoT), Bluetooth, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), ZigBee, and 5G NR New Radio (NR), Since network security is a major concern in healthcare, processing data at the edge instead of relying entirely on cloud computing helps reduce

latency, minimize privacy risks, and enhance real-time monitoring of critical patient data [18],[19].

- Application Layer: Acts as an interface for end-users and healthcare professionals, enabling access to patient data, monitoring, and resource management, essential for delivering healthcare services [20].

Other studies show that the IoMT systems consist of three levels:

1. **Device:** Sensors and IoMT devices.
2. **Edge node:** Helps IoMT devices by providing extra processing and storage power, allowing smart data analysis to happen closer to where the data is generated instead of relying only on distant cloud servers. Examples include smartphones and gateways, which in our work are located inside the ambulance.
3. **Cloud:** Offers powerful processing and virtually unlimited storage, enabling the registration and secure management of all medical devices and edge nodes by storing their real identities [3],[12].

2.3 Attack Model

IoMT device-driven health systems are increasingly under threat of cyberattacks due to the many entry points and layers in their architecture. These attacks can target different parts of the system to steal or modify sensitive medical data or even cause harm to patients and hospitals. Each layer in the system has its own set of security challenges. For example, DoS and DDoS attacks are applied against the denial of access to healthcare services by saturating the network or devices. Man-in-the-Middle (MitM) attacks target stealing or compromising data as it is moved between devices, especially at the edge or network levels. At the application layer, attacks such as sniffing and access control attacks are common. Ransomware and malware attacks primarily affect the storage and cloud layers, resulting in data loss or corruption. Other attacks, like injection and password-based attacks, attempt to bypass login systems and user access controls [10],[21]. A summary of most of these attacks and their potential impact on healthcare IoMT environments is provided in Table 2.1 and 2.2.

Table 2.1: Common Cyber-Attacks in IoMT Environments

No.	Attack Type	Description
1	MitM Attacks	This refers to a type of cyber-attack involving an attacker intercepting communication between two parties undetected and modifying it, making it possible for this attack to have serious implications within IoT or IoMT environments to eavesdrop or manipulate data undetected [61].
2	Ransomware Attacks	The aim of ransomware attacks is to prevent users from having any form of access to their files on the computer through encryption while paying a ransom. This is a major concern in hospitals due to the economic costs associated with such attacks [62].
3	Injection Attacks	An injection attack happens when attackers launch their attacks through communication channels involving IoMT devices, which may include fictitious oxygen saturation values for example. This may result in erroneous patient diagnosis or inappropriate medical interventions. In other instances, attacks target the transmission of malware, resulting in compromised medical equipment or unauthorized access to personal healthcare information [63].
4	Malware Attacks	Attackers gain system access, and malicious acts such as crashing, modifying, spying on, or deleting system or data files and folders are possible by exploiting vulnerabilities in the device protocol system to install malware [21].
5	DDoS Attacks	A device and/or network is flooded with spurious requests, thereby rendering it unusable. Deny of Service attacks are very important in a hospital setting where downtime can be potentially life-threatening [64].

Table 2.2: Common Cyber-Attacks in IoMT Environments

No.	Attack Type	Description
6	Phishing Attacks	Phishing is a method of attempting to acquire potentially valuable pieces of information, such as usernames, passwords, or medical data, for malicious purposes by means of targeted communications, including emails and instant messaging in which the malicious party attempts to induce victims to click on links to malicious websites or download malware [71].
7	Medical Data Tampering Attacks	Medical data tampering refers to the unauthorized modification of medical data, where the attacker changes the content of medical information such as medical images, electronic health records, and sensor readings, which results in incorrect interpretations of the medical data [72].
8	Data Poisoning Attacks	Data poisoning attacks happen when an attacker injected malicious or manipulated samples into the training dataset in an attempt to poison the learned model and produce incorrect predictions during deployment [73].
9	Third Party Attack	Third parties, such as vendors and contractors, may also need to have access to the system, which poses a security risk, as an attacker can use this to gain access to a number of healthcare organizations with a single attack [74].
10	Cloud Account Attack	Cloud Account Attack is an attack where attackers target cloud users' or administrators' accounts through weak authentication, stolen credentials, and/or misconfiguration, resulting in unauthorized access to sensitive information and services. This type of attack may result in data breaches and misuse, considering that cloud environments are prone to account and access control vulnerabilities [75].
11	Data Breaching	In the healthcare sector, a data breach is referred to as the unauthorized acquisition, access, use, or disclosure of protected health information, which violates the privacy or security of the health information [76].

Most attacks have been addressed in previous studies. In this work, we specifically focus on two attack types: injection and DDoS. The study further integrates the ZTM with injection attacks to enhance security, prevent unauthorized data manipulation, and improve the overall resilience of IoMT systems against such threats especially in the case of smart ambulances, Other attack modes can also be integrated and implemented in a similar way in this layer.

2.4 Integration of Advanced Technologies in EMS System

2.4.1 The Zero Trust Model (ZTM)

It is a cybersecurity model that, while not new, has gained significant traction in recent years. It was first introduced by John Kindervag in 2010 [22] when he was working as a principal analyst at Forrester Research. The idea behind it starts from the assumption that threats can come from anywhere, either inside or outside. Instead of trusting users and devices by default, zero trust is an approach of "Never trust, always verify [23]. It is an intelligent approach that continuously verifies the user's identity and permissions before granting resource access, regardless of location or network. Access is temporary and requires regular revalidation, forming the key principles of ZTM [24] as illustrates in Figure 2.2:

A. Never trust, always verify: Thus, the general principle by default is that no user, device, or network is to be trusted, even in the security perimeter. Any access request must be authenticated and authorized before access is approved.

B. Least Privilege Access: Grants users only the minimum access needed for their tasks, limiting potential damage if an account is compromised.

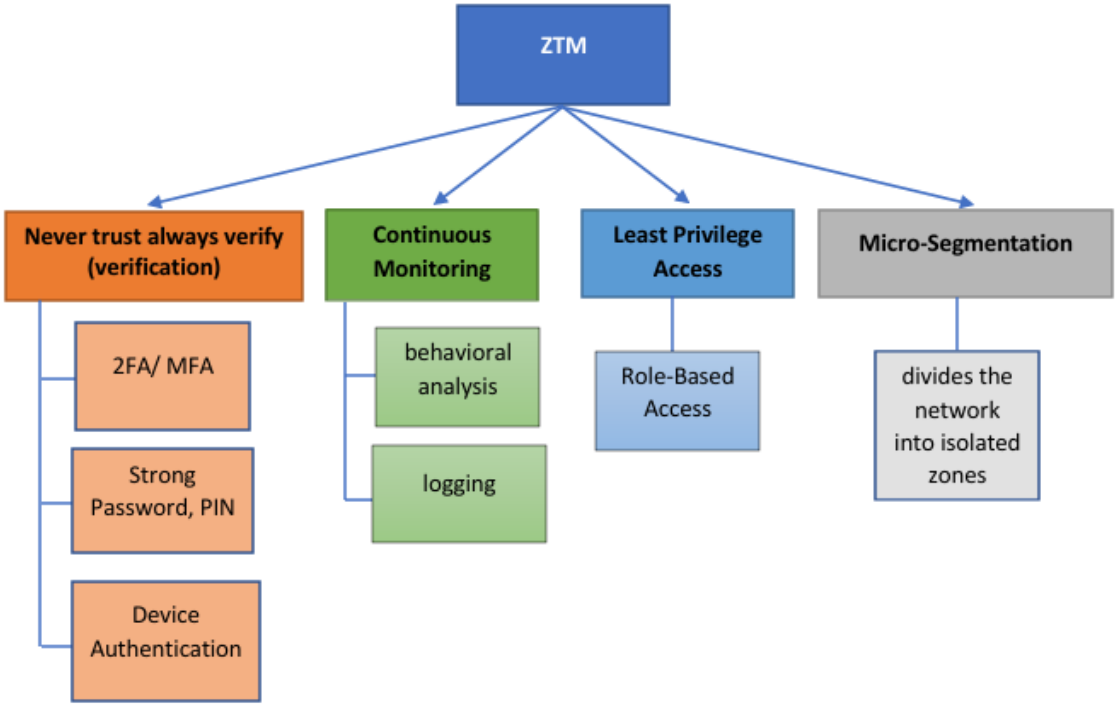

Figure 2.2: ZTM General Principles

C. Micro-Segmentation: Micro-segmentation divides the network into isolated zones, limiting an attacker's lateral movement and minimizing potential impact.

D. Continuous Monitoring and Validation: Detecting unusual activities after behavioral analysis and logging instead of assuming granted access is always safe.

The importance of ZTM lies in its operating principle: never trust, always verify. This reduces external and internal risks that threaten the system, re-

quiring continuous verification and monitoring, and also isolating the source of the threat.

2.5 Two-Factor Authentication (2FA)

It refers to an identity and access management security mechanism that requires two categories of identification for the use of resources and information [25]. Authentication factors can generally be classified into three traditional categories as follows [26]:

- Something known (password, pattern, etc.).
- Something owned (smart cards, OTP, etc.).
- Something inheritable (biometric, fingerprints, behavioral pattern, etc.).

Different authentication methods exist, such as Single-Factor Authentication (SFA), 2FA and Multi-Factor Authentication (MFA). This would mean that as the factors increase, the security will be improved to give data more protection. This research will focus on 2FA to balance security and usability. We will enhance security by incorporating additional mechanisms, including ML, zero trust, and SIDS, to strengthen security further and safeguard sensitive information. Significantly minimize the risk of security breaches in IoMT devices.

2.6 Intrusion Detection System (IDS)

It is an active security component that monitors and inspects system or network traffic to detect vulnerabilities and threats. IDS is always vigilant for user information, network, and service traffic to detect unauthorized access and extend integrity,

confidentiality, and availability (CIA) to information systems. IDS plays a pivotal role in network security, especially in IoMT, as it helps prevent and detect different classes of known attacks [27].

In general, IDS can be categorized in two ways, as illustrated in Figure 2.3:

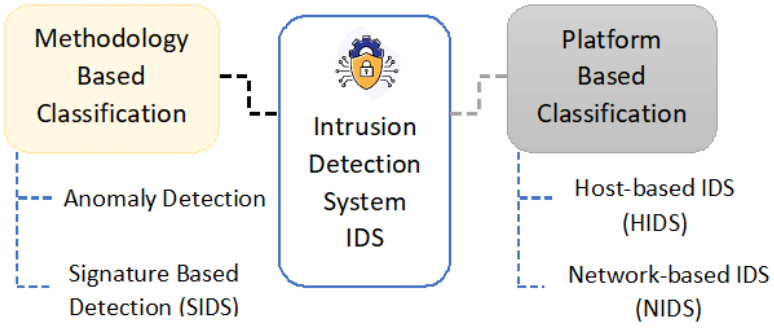

Figure 2.3: Intrusion Detection Methodologies

- Classification by methodology.
- Classification based on the platform being monitored.

IDS can be classified as anomaly-based and signature-based detection. Anomaly-based detection learns normal behavior and alerts when deviating, which has the capability to detect zero-day attacks. It is difficult for it to accommodate changes and tends to produce high false positives. In contrast, signature-based detection compares events to known attack signatures called SIDS, with higher accuracy and fewer false positives, but cannot detect unknown attacks [28]. In our proposed model, we used SIDS when training the model on the cloud to determine the specific intru-

sion at the data content level.

In IoMT, ambulance-based emergency medical services rely on IoMT devices to monitor patients' vital signs and transmit real-time data to hospitals. However, these systems face security threats like DoS/DDoS attacks, which can disrupt data transmission and delay ambulance vehicles.

Study [29] classifies cyber-attacks on intelligent vehicles, including ambulances, into two main types: in-vehicle threats targeting onboard systems like devices patient data, and network threats. This research adopts that classification in the context of ambulances, focusing on two threat levels: data content and network communication level. This layered approach supports the proposed system's ability to detect cyber threats and secure real-time transmission of vital signs at two levels.

2.7 Machine Learning

Organizations are increasingly turning to Artificial Intelligence (AI) to withstand emerging cybersecurity threats, technological problems, lack of resources, and increasing system strength [35]. ML, which is a branch of AI, enables machines to be trained on data without explicit programming. Active ML is effective for complex problems that classical solutions find challenging and fits new data nicely. From research, it is shown that ML in Intrusion Detection System (IDS) can effectively detect zero-day attacks and vulnerabilities, while rule-based IDS can detect known attacks. Current work highlights the requirement for feature selection and pre-processing to

improve attack detection. Four categories of ML types illustrated in Figure 2.4 can be utilized to solve EMS security issues [30], [31].

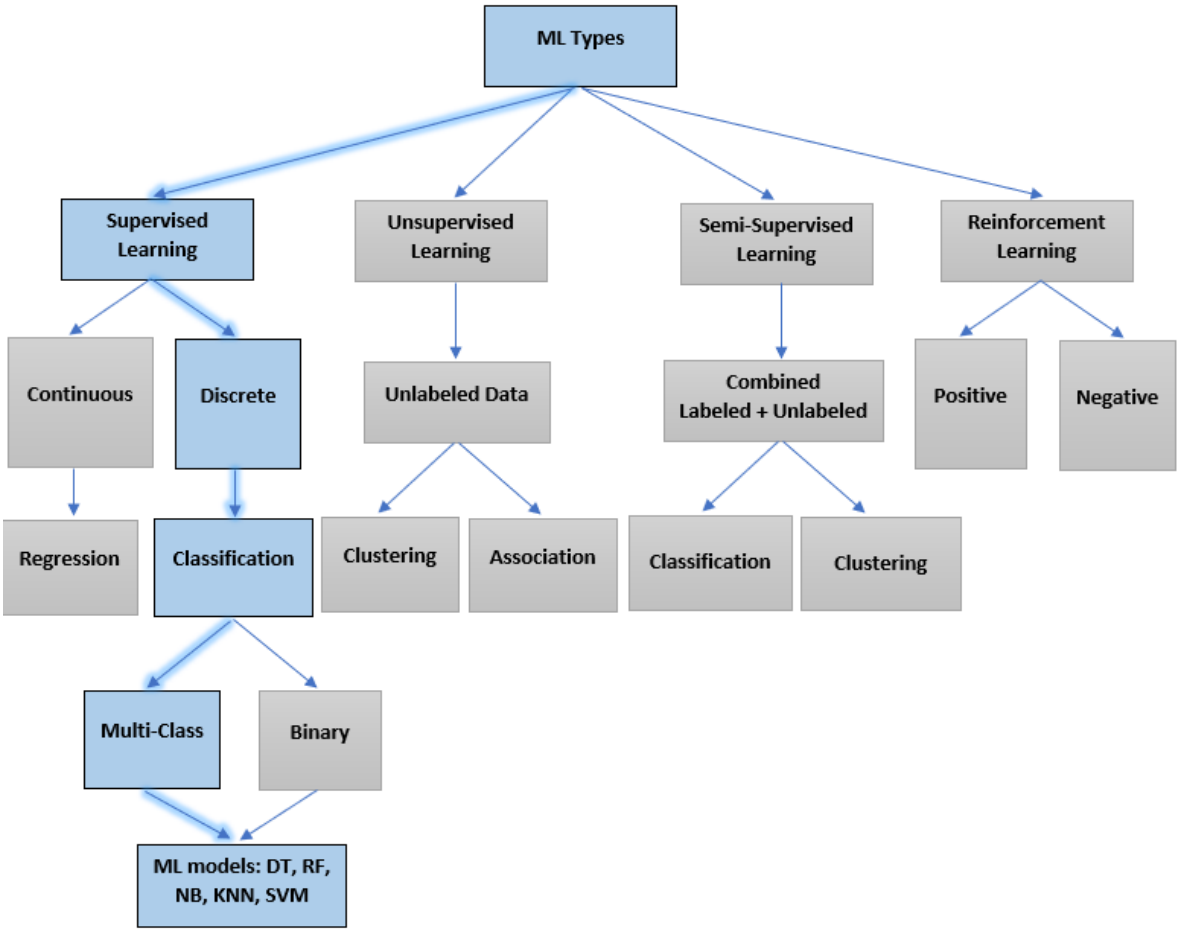

Figure 2.4: Overview of Machine Learning Types

- Supervised Learning: This detects the known attacks, which have labeled data.
- Unsupervised Learning: It identifies anomalies from normal behavior without labels.
- Semi-Supervised Learning: Combines both to handle limited labeled data.

- Reinforcement: Models are based on reward or penalty (positive/negative).

The figure illustrates an overview of the main categories of ML. The highlighted path in blue represents the focus of this research, specifically supervised learning with discrete outputs, such as classification tasks. Specifically, this work addresses multi-class classification, where the output can belong to more than two categories. The selected ML models for this task include DT, RF, and KNN.

2.8 ML Models Used

This section provides an overview of the ML models employed in this research, briefly discussing their major mechanisms . The models DT, RF, and KNN were selected as a result of their impressive performance in classification, low computational overhead, and real-time decision-making capability, which are appropriate in IoMT environments.

2.8.1 Decision Tree

Decision Tree is a supervised learning algorithm that is used for classification and regression; it builds a tree-like decision model based on feature values. It is an easy structure to understand and follow. Some decision tree algorithms are also used in user behavior analytics and cybersecurity analytics [31].

The working principle of a decision tree is as follows [31]:

1. Starting at the root node, where the model selects a feature to evaluate.

2. At each internal decision node, a specific attribute of the input instance is

checked.

3. The model follows the branch corresponding to the observed value of that attribute.

4. This decision-making process is repeated recursively through the tree

5. When a leaf node is reached, it provides the final prediction (class label), and the process is rule-based and hierarchical, which makes the model interpretable and easy to trace.

Splitting criteria are based on impurity measures that evaluate how effectively a feature separates the classes at each node. The two most common metrics are [31]:

1. Gini Impurity: The Gini impurity Gini(E) measures the probability of incorrectly classifying a randomly chosen element if it was labeled according to the class distribution in the node. It is calculated as shown in Equation (2.1) :

$$Gini(E) = 1 - \sum_{i=1}^{c} p_i^2 \tag{2.1}$$

Where:

- E is the dataset at the current node
- c is the number of classes
- p_i is the proportion of instances belonging to class i

A lower Gini value indicates a purer node.

2. Entropy and Information Gain: Entropy measures the disorder or impurity within a node. It is calculated as shown in Equation (2.2):

$$Entropy(S) = -\sum_{i=1}^{c} p_i \log_2 p_i \tag{2.2}$$

Where:

- S is the dataset at the current node
- c is the number of classes
- p_i is the proportion of instances of class i in the dataset

A lower entropy value indicates a purer node, while a higher entropy suggests more class mixing.

Information gain quantifies the reduction in entropy after splitting the data on a particular feature. It is calculated as shown in Equation (2.3):

$$Gain(S, A) = Entropy(S) - \sum_{v \in Values(A)} \frac{|S_v|}{|S|} \cdot Entropy(S_v) \tag{2.3}$$

Where:

- A is the feature to split on
- $Values(A)$ is the set of all possible values of attribute A

- S_v is the subset of dataset S for which feature $A = v$
- $|S|$ is the total number of instances in the dataset
- $|S_v|$ is the number of instances in subset S_v

The feature with the highest information gain is selected for splitting at the node.

The following are advantages and limitations of the DT model [32]:

Advantages of Decision Tree

- The DT model is efficient and easy to interpret. It requires minimal data preprocessing, as it can handle missing values and both numerical and categorical data. It also offers logarithmic prediction cost and supports multi-output problems.

Limitations of Decision Tree

- DT can easily overfit the data by creating complex trees that do not generalize well. It is also unstable to little changes at the data, leading to different tree structures. Its predictions are piecewise constant, limiting extrapolation, and some patterns like XOR are difficult for DT to represent effectively.

2.8.2 Random Forest

Random Forest Model: It is a parallel ensemble classification learning algorithm that builds multiple decision trees using bootstrap samples and features and combines

their outputs to improve accuracy and reduce overfitting, which has three main parameters [31],[33]:

1. Node size.
2. Number of trees.
3. Number of features sampled.

Figure 2.5 illustrates an example of RF consisting of multiple DT. The working principle of an RF is as follows [33]:

- Ensemble Model: RF is an ensemble learning model, which means it builds multiple decision trees and combines their predictions to produce a final output.
- Bootstrap sampling: Every tree is trained on a random subset of the training data with replacement; this is called a bootstrap sample.
- Out-of-Bag (OOB) data: About one-third of the data are not included in each bootstrap sample and are used later for internal cross-validation.
- Feature bagging: At each node split instead of using all features, a random subset of features is selected, which increases diversity between trees.
- Parallel training: The decision trees are all independent and in parallel, which speeds up training and helps avoid the overfitting.
- Prediction process:
  - Classification tasks: The final output is based on majority voting.

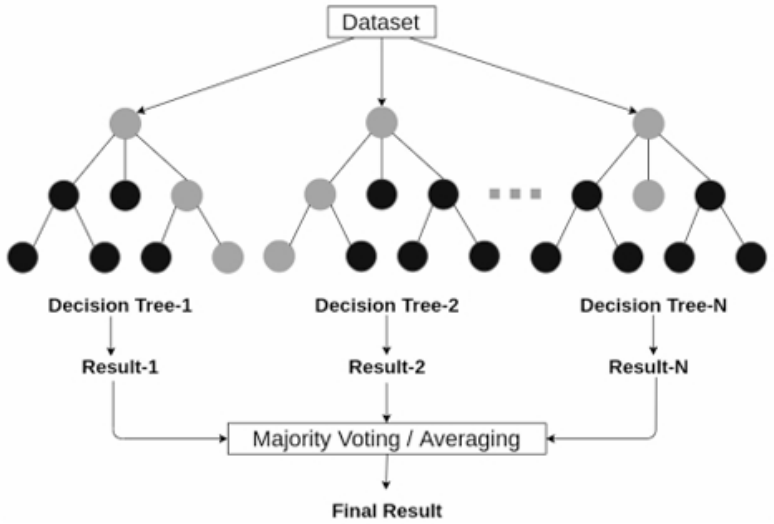

Figure 2.5: An example of RF consisting of multiple DT [31]

- Regression tasks: The final output is the average of all tree predictions.
- Final evaluation: The OOB samples are used to estimate model accuracy without needing a separate validation set.

The following are advantages and limitations of the Random Forest model [33]:

Advantages of Random Forest

- It also offers logarithmic prediction cost, supports multi-output problems. An RF model can reduce the risk of overfitting because it combines several uncorrelated trees and averages the outputs, which lowers the variance and leads to improved generalization. It is flexible; it handles both classification and regression tasks with good accuracy and can deal with missing data. RF also provides a simple way to measure feature importance using Mean Decrease in

Impurity (MDI) and Mean Decrease in Accuracy (MDA)methods.

Limitations of Random Forest

- Time-consuming: Because the RF model can handle large data sets, it can be provide more accurate predictions but can be slow to process data as it is computing data for each individual DT.
- It's a more complex prediction compared with DT and requires more resources to store the data.

2.8.3 K-Nearest Neighbors

It is a supervised ML model that can be used for classification or regression problems; the classification depends on the proximity of individual data points, working on the assumption that all similar points can exist near one another [34].
The working mechanism of a K-Nearest Neighbors is as follows [34]:

- Storing the training data: In this model, there is no need for traditional training; instead of that, it stores the training dataset and performs all computations at the time of prediction.
- Select the number of neighbors (k): The programmer or user should determine the value of K; the smaller value of K could be sensitive to noise, rather than the larger value of K, which can reduce the sensitivity of the model.
- Calculate the distance between the new input and all training samples: There are many equations based on similarity measures used to determine how close

each training sample is to the new data point. The two most commonly used equations:

1. **Euclidean Distance**: It is the most common distance measure, which measures the straight-line distance between two different points in a multi-dimensional space. The Euclidean Distance for x and m is defined in equation (2.4).

$$d(x, m) = \sqrt{\sum_{i=1}^{n}(x_i - m_i)^2} \tag{2.4}$$

Where:

- x and m: Two data points to compare.
- x_i and m_i: The i^{th} feature values of x and m, respectively.
- n: The total number of features.
- $d(x, m)$: The Euclidean distance between the points x and m.

This equation is the most common distance metric that is used in the KNN model. It measures the straight-line distance between two different points in a multi-dimensional space.

2. **Manhattan Distance**: This is another commonly used measure of distance, which measures the absolute difference between two points. The Manhattan Distance for x and y is defined in equation (2.5).

$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{2.5}$$

Where:

- $d(x, y)$: The Manhattan distance between the two data points x and y.
- $|x_i - y_i|$: The absolute difference between the i^{th} feature values of x and y.
- n: The total number of features (dimensions).

The following are advantages and limitations of the K-Nearest Neighborst model [34]:

The advantages

- Easy to apply: Due to the ease and efficiency of the algorithm, it is one of the first classifiers that a new data scientist would learn.
- Highly adaptable: Since KNN stores the entire training dataset in memory, it can easily incorporate new training samples without retraining, allowing it to adapt to new information quickly.
- Little parameters used: The only parameters required by KNN are the k parameter and a distance measure, which are fewer than other machine learning algorithms.

The limitations

- KNN suffers from high memory usage and slower performance since it stores all training data and computes predictions at runtime. It also faces the curse of dimensionality, where high feature counts reduce accuracy, and is prone to

overfitting with small k values or underfitting with large ones, making proper k selection essential.

2.9 Summary

This chapter gives an introduction to the architecture of the IoMT systems in general, explains the concept of attack models, and demonstrates that attacks can target different parts of the IoMT system inside the ambulance, including devices, networks, and data transmission.

Also explains the integration of various technologies in the EMS system, including ZTM, 2FA, and SIDS, to detect the specific attacks: DDoS at the networks and injection into data content after analays their behavior.

Additionally, a brief overview of ML models used in the thesis and an explanation of the advantages and limitations of each one: DT, RF, and KNN.

Chapter 3

Literature Review

In this chapter, we present a literature review related to the core of the work, divided into four categories: cybersecurity for mobile medical environments, cybersecurity for static medical environments, multi-layered security models, and edge-deployed lightweight security models for IoMT. The comparisons are based on different aspects close to the work.

In a recent comprehensive review, the authors in [4] examined the growing field of IoMV and highlighted its specific security and privacy challenges. The study pointed out that, despite the increasing use of smart mobile healthcare systems like ambulances, the research focused on securing these environments is still limited. It reviewed several types of possible attacks on IoMV systems, such as DoS attacks, data manipulation, and unauthorized access. The authors emphasized the need for new security frameworks that support real-time threat detection, lightweight encryption,

and multi-layered access control. They also called for further research into integrating technologies like IDS, ML, and authentication mechanisms to build more proactive and adaptive security solutions. These findings closely align with the direction of this thesis, which proposes a real-time, multi-layered security framework specifically designed for EMS environments.

The four categories each present a group of related previous studies. Some studies may appear in more than one category but are analyzed from different comparative perspectives in each case.

3.1 Cybersecurity for Mobile Medical Environments

This category contains a collection of studies, some of which are recent, on the security of vehicles in general, which are connected to the internet, including ambulances.

3.1.1 Employing the Beamforming Technique to Enhance the Medical Ambulance Performance, IoMT

The researchers in this paper [36] aimed to improve the operation of medical ambulances in real-time and healthy safety areas through the utilization of beamforming technology in 5G communication networks. Key agreement protocols were incorporated into the utilization of 4G/LTE or 5G as access technologies to protect data transfer from cyber threats. The study did not address the specific steps that must be followed in the event of a health cyberattack, nor did it sufficiently focus on the protection and security of the transferred medical data. The analysis and detection of attacks, which is the primary focus of this thesis, is not addressed in the referenced system, meaning it cannot determine whether a breach or data tampering has

occurred.

3.1.2 Smart Ambulance for Emergency Cases to be Reported to Hospitals at the Earliest using Deep Learning Algorithms and Blockchain-based Distributed Health Record Transactions for Smart Cities

The authors of the paper [38] proposed a smart ambulance system for emergency cases in smart cities, integrating deep learning algorithms and blockchain-enabled distributed health. The deep learning algorithms were used to predict patient injuries, and blockchain technology ensured security, privacy, and health data integrity during transmission. The article covers the real-time emergency case transmission via a blockchain-secured channel to provide integrity of data during transmission. But in this case, if the medical device itself is hacked or cloned, the medical data issued by it will be transferred as is.

3.1.3 A Modular In-Vehicle C-ITS Architecture for Sensor Data Collection, Vehicular Communications and Cloud Connectivity

The study [37] introduced an entire system to collect sensor data from smartphones and vehicles and transmit them to the cloud using Message Queuing Telemetry Transport (MQTT), but the security concerns of the communication are not discussed. The focus was on the architecture and data transmission in the context of an Internet of Vehicles (IoV) environment, without focusing on important issues such as data protection, attack detection, or preserving the integrity of communication. In contrast, our study builds on such systems by incorporating security mechanisms and intelligent detection techniques specifically tailored for smart ambulances and IoMT

environments operating within the IoV system.

3.1.4 Smart Ambulance with Patient Health Monitoring

The study in paper [9] describes an intelligent ambulance system using IoT technology to monitor vital signs and transmit real-time data to the hospital. It also improves traffic flow by remotely controlling traffic lights. The system reduces response time and aids doctors in making quicker, more accurate medical decisions. The security tools in this paper, which could be used to transfer critical patient data through this ambulance system, were not addressed.

Table 3.1 presents a classification and comparison of four selected studies related to cybersecurity in mobile healthcare environments. The table highlights differences in their main ideas, datasets, security tools, methodologies, and results. As shown, these studies did not focus on real-time threat detection, but instead applied protection mechanisms such as blockchain and security protocols.

Table 3.1: Cybersecurity for Mobile Medical Environments Summary

Ref	Year	Main Ideas	Dataset Used	Security Tools/ Approaches	Methodology	Results
[36]	2025	Improve the performance of medical ambulances in real-time using the beamforming technique of 5G. Integration of IoMT and telemedicine to reduce data transmission latency and enhance patient care.	No real dataset; simulation only	5G key agreement protocols; Low-power secure transmission; Neural networks to secure multimedia; communication protections between vehicles	Simulated smart ambulance system with 3D-beamforming, 5G, V2X across urban/rural scenarios. Antenna and mobility modeled in 28GHz mmWave band.	Faster data transmission; Better ambulance–hospital coordination; Improved patient tracking; Less communication delay
[38]	2024	Proposes a Smart Ambulance system for early emergency case reporting using deep learning and blockchain to support distributed health record transactions in smart cities.	Not specified	Blockchain-based authentication; Privacy preservation; Data integrity	Deep Learning (CNN and LSTM) for emergency detection; Blockchain for secure medical data handling and transaction validation	Improved emergency reporting time and more reliable medical data exchange via blockchain integration
[37]	2023	Proposes a modular in-vehicle C-ITS system to collect sensor data from OBD-II and smartphones, and transmit it to the cloud for real-time road condition monitoring in IoV environments.	Real-world data from sensors collected during road tests in Portugal	Not addressed. Focused on system architecture and data communication.	Hardware prototype using Carloop and RedBear Duo; real traffic tests with CAN and smartphone sensors; data transmitted via MQTT to cloud; reverse engineering used for parameter detection.	Successfully collected and transmitted sensor data; enabled real-time monitoring of road conditions; improved awareness of environmental and driving context.
[9]	2020	Proposes an IoT-based smart ambulance system integrating patient health monitoring and traffic signal control to improve emergency response.	Real-time sensor data collected using temperature and heart rate sensors during testing; results shown on LCD and sent to server; includes example test cases.	Not addressed	Implementation using biomedical sensors, joystick-controlled signaling, microcontrollers, and ESP8266 Wi-Fi module; data sent to a 24/7 hospital web interface.	Enabled early communication of patient condition to hospitals and traffic signal control; improved emergency response time and hospital readiness.

3.2 Cybersecurity for Static Medical Environments

This category contains a collection of studies, wich use security tools at static environments, like hospitals and homes, to protect patient data or IoMT devices or the networks.

3.2.1 Intelligent two-phase dual authentication framework for Internet of Medical Things

In this paper [41], a two-phase dual authentication protocol is proposed for enhanced security in IoMT static environments. It uses Elliptic Curve Diffie-Hellman Elliptic Curve Diffie-Hellman (ECDH) for fast key exchange during the registration process and AES-GCM encryption for real-time data safety. The simulation results show significant improvement over state-of-the-art methods, reducing encryption/decryption time, computational cost, and latency. The model has strong defenses against different attacks, such as man-in-the-middle, replay, and brute force attacks, ensuring the confidentiality and integrity of medical data.

3.2.2 Continuous and Mutual Lightweight Authentication for Zero-Trust Architecture-Based Security Framework in Cloud-Edge Computing-Based Healthcare 4.0

In the paper [6], they propose a lightweight continuous mutual authentication protocol based on ZTA for Device-to-device (D2D) and Device-to-Edge (D2E) communication security in healthcare 4.0 systems: Hash-based Message Authentication Code (HMAC), while Edge-to-Cloud (E2C) used Elliptic Curve Cryptography-Advanced Encryption Standard (ECC-AES) for authentication and Identity-Based

Access Control (IBAC) for authorization access. Compared to this work, they work on ZTM based on authentication; in contrast, we used ZTM based on behavior analysis. Our method trains ML models in the cloud to address limited resources for this system and then deploys them at the edge for real-time detection with high-security performance.

3.2.3 ZTCloudGuard: Zero Trust Context-Aware Access Management Framework to Avoid Medical Errors in the Era of Generative AI and Cloud-Based Health Information Ecosystems

The authors at the paper [39] proposed a zero-trust access control system designed for static healthcare environments such as hospitals and cloud-based platforms. The main objective was to reduce medical errors caused by authenticated users or AI-assisted decisions by integrating security tools like authentication, authorization, encryption, and logging alongside pre-trained machine learning models for semantic and syntactic data analysis. The system achieved good effectiveness, indicating how it can reduce medical errors in cloud-based healthcare systems. In contrast, our proposed system applies ZTM at the edge, specifically within mobile and sensitive environments such as ambulances, enabling real-time data processing and securing critical patient information before it reaches the hospital, thereby enhancing the protection of vital signs during transit.

3.2.4 Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection

An optimized real-time detection IDS for network traffic features at IoMT systems was proposed [40] using tree-based machine learning classifiers and filter-based feature selection techniques. The proposed model is used for monitoring and identifying unauthorized or malicious activities within medical devices and networks. The paper was based on the CICIDS2017 dataset, showing an accuracy of 98.79% and a very low false alarm rate of 0.007. Thus, the model was proposed in terms of less computational complexity, and detection precision was foreseen as very strong, with much potential for ensuring security within IoMT environments. However, while their model detects unauthorized activities via network traffic features, our system adds medical data analysis to detect spoofing attacks on compromised devices. This dual-layer approach enables distinguishing cyberattacks from real medical issues in critical, mobile IoMT settings like ambulances.

Table 3.2 presents a classification and comparison of four selected studies related to cybersecurity in static healthcare environments. The table highlights differences in their objectives, areas focus, use of AI/ML, tools used, and detection time. As is clear, most studies have focused on applying security to static healthcare environments like hospitals and have been applied at more than one level. This contrasts with the previous group of studies in mobile healthcare environments such as ambulances, where relevant research remains limited.

Table 3.2: Comparison of four selected studies related to cybersecurity in static healthcare environments

Ref	Year	Study Objective	Focus	Use ML/AI	Environment	Tools Used	Detection Type
[41]	2025	Enhance the security of communication in IoMT and protect sensitive medical data transmitted	Data and Network	No	Hospital	- ECDH for registration phase - AES-GCM for data encryption	Real-Time
[6]	2024	Proposes ZTA-based lightweight framework with continuous mutual authentication for D2D and D2E communications, and IBAC for secure E2C access control.	Data transmissions among: Device, edge, and cloud	No	Hospital	ZTM based continuous authentication strategy: HMAC, IBAC and ECC-AES	Real-Time
[39]	2024	Reduce medical errors caused by authenticated users or AI assisted decision.	Cloud ecosystem, including users, devices, and output data	AI	Cloud	Zero-trust access control, encryption, and logging	Pre-trained
[40]	2024	Monitoring and identifying unauthorized or malicious activities within medical devices and networks	Medical devices and networks	ML	Hospital	IDS with tree-based machine learning classifiers, and filter-based feature selection techniques	Real-Time

3.3 Multi-Layered Security Models

Multi-layered security models need to apply multiple security mechanisms across many layers of the system structure, including the network, data, user, and device.

This approach enhances overall resilience by ensuring that when one layer is breached, there are others that remain protected. Studies under this category typically combine tools like encryption, authentication, and access control across these layers in an effort to provide comprehensive protection.

3.3.1 Secure Latency-Aware Task Offloading Using Federated Learning and Zero Trust in Edge Computing for IoMT

In this paper [43], a multi layered IoMT security framework called Trust and Latency-aware Task Offloading (TLTO) involving ZTM integrated with Federated Learning (FL) is proposed in this work to ensure robust privacy and security in the decentralized IoMT static environment. The architecture includes layered protection across the device, communication, edge, authentication, and cloud levels. It employs lightweight authentication at the device layer and enables secure, latency-aware task offloading.

3.3.2 Intelligent Two-Phase Dual Authentication Framework for Internet of Medical Things

The authors [41] proposed a two-stage authentication framework in this study employs security at multiple levels. They apply ECDH to secure the network layer through safe key exchange, while AES-GCM encryption protects the data layer by ensuring confidentiality and integrity. At the application layer, they use a two-phase dual authentication mechanism that is implemented to continuously verify the device and user.

3.3.3 Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection

The model [40] optimized real-time detection IDS for network traffic features at IoMT systems. This proposed model is used for monitoring and identifying unauthorized or malicious activities within medical devices and networks. This dual-layered approach enhances overall IoMT system security by balancing local efficiency with global threat detection.

3.3.4 Multi-layer security scheme for implantable medical devices

In this paper [42] the proposed solution offers an multi-layer security model for Implantable Medical Devices (IMDs) with an electrocardiogram (ECG)-based authentication system. The design safeguards three crucial layers: Data, network, and application, while keeping functionality lightweight for compliant IMDs with limited resources. It boasts a significant up to 99.99% accuracy rate in identifying authorized users, indicating high reliability as well as efficiency. While most existing solutions target static or hospital environments, there is limited research addressing multi-layer security for mobile environments.

Table 3.3 summarize comparison of previous studies in healthcare system generally static or mobile which focus on multilayer security models include: layer of application, dataset used, attack focus ,environment, and the result and evaluation.

Table 3.3: Multi-Layered Security Models Summary

Ref	Year	Layer of Application	Dataset Used	Deployment Location	Attacks Focus	Results
[43]	2025	Multi level Device, Edge device, Network	Not Specified	Hospital	Identity spoofing, MITM, Sybil attacks	- Higher task success rate - Improved energy efficiency - Strong protection against unauthorized access.
[41]	2025	Network, Data, Application	Not Specified	Hospital	MITM, Replay, Brute Force	The performance improvements include a 45% reduction in encryption/decryption time, a 45.38% decrease in computational cost, and a 28.42% drop in latency compared to existing methods.
[40]	2024	Device and Network	CICIDS2017 dataset	Hospital	DDoS, Brute Force, DoS, Web Attack, Infiltration, Botnet, and Port Scan.	The model reached s 98.79% accuracy and a low false alarm rate 0.007, indicating highly effective intrusion detection at both device and network levels.
[42]	2020	Multi level layered (Network, Data, Application)	ECG Data	Hospital	Not Specified	The model demonstrated high accuracy, achieving up to 99.99% in identifying authorized personnel, even with a limited number of coefficients

3.4 Edge-Deployed Lightweight Security Models for IoMT

Recent studies show that IoT systems in healthcare need simple data collection and visualization. They are now becoming intelligent systems capable of analyzing data and making the medical decisions. This is founded on AI and ML, which are often run in the cloud. However, relying entirely on cloud computing introduces issues such as delays in response times, internet dependency, and data privacy concerns. To alleviate these limitations, recent approaches utilize edge and fog computing to move decision-making close to the data source. This improves response time and system performance, especially in time-sensitive for medical applications [44].

This category contains some studies that deploy the security models at the edge computing node.

3.4.1 Secure Latency-Aware Task Offloading Using Federated Learning and Zero Trust in Edge Computing for IoMT

The emphasis of this paper [43] is on edge computing for the processing of time-sensitive medical operations. The proposed TLTO model enables secure and efficient task execution across resource-constrained edge nodes. Achieved by leveraging lightweight cryptographic methods, the framework minimizes latency while preserving data privacy.

3.4.2 A Hybrid Fog-Edge Computing Architecture for Real-Time Health monitoring in IoMT systems with optimized latency and threat resilience

In this study [45], the authors proposed a hybrid fog-edge computing which designed for real-time health monitoring in IoMT systems. The targets of the model are to reduce latency and ensure greater data security for patients by processing critical health data close to the source using lightweight machine learning models and multi-layer encryption. Latency was reduced by 70% and threat identification was significantly faster compared to cloud-based systems. Although the study was done using statical environments like hospitals and homes, its design and findings are suitable for comparison with mobile medical environments, such as ambulance.

3.4.3 An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems

In paper [46], they proposed an effective training scheme for deep neural networks DNN within edge-computing-enabled IoMT systems. The proposed model aimed at enhancing real-time disease diagnosis by processing the patients' data locally at the edge, hence enhancing latency and preserving privacy. The solution recognizes the potential of edge-based intelligent processing for efficient, timely, and secure medical decision-making.

Table 3.4 presents comparason between 3 studies in the healthcare system sector focussing on edge/edge-fog deployments due to the latency and privacy issues at the cloud. Also, the internet dependency, these studies show the importance of this

mechanism and how it reduces the latency and makes the decision-making in real time close to the data source, which appears a reason to apply our work at the edge.

Table 3.4: Edge-Deployed Lightweight Security Models for IoMT Summary

Ref	Year	Motivation	Method	Advantages	Disadvantages	Results
[43]	2025	IoMT demands low-latency and secure processing, and cloud reliance may create privacy and delay concerns. Therefore, edge offloading is vital for time sensitive healthcare operations.	A TLTO framework designed to secure real-time task offloading in IoMT using a combination of FL and ZTA.	Low Latency, Privacy-Preserving, Real-Time Response	Edge environments face security and trust issues, especially when offloading tasks to potentially untrusted nodes.	- Higher task success rate - Improved energy efficiency - Strong protection against unauthorized access.
[45]	2025	Cloud-based IoMT systems face high latency and security risks, making real-time processing essential for critical medical situations.	Hybrid Edge–Fog model with real-time anomaly detection using lightweight ML (DT, One-Class SVM), then evaluated simulation tools (Fogify, NS-3).	latency reduction and energy savings also fast security threat detection (30ms)	Requires constant maintenance and model updates and high infrastructure cost	Security threats are detected in 30 ms, and there is 99.5% health anomaly detection accuracy, as well as 30% improvement in energy efficiency.
[46]	2020	It proposes using Edge AI to overcome high latency, privacy risks, and high resource at the cloud and improve smart healthcare efficiency.	It involves collecting vital signs from IoMT devices and processing them locally at the edge using lightweight neural networks.	Reduced latency, improved diagnostic accuracy, and lower energy and bandwidth consumption. It also enhances privacy by processing data locally without relying on the cloud.	Resources are limited, which restricts the size and complexity of neural network models.	Edge neural networks were 94% accurate in the detection of medical conditions, with a 40% faster response time than cloud processing. Data privacy was above 90% since data wasn't sent to a central server.

3.5 Literature Review Conclusion

While the reviewed literature gives valuable insights into securing IoMT systems environments, only a limited number of studies have addressed mobile healthcare environments, such as ambulances. A recent study emphasized the lack of adequate security mechanisms in these dynamic environments lack optimal security measures to explore solutions tailored for such use cases. Moreover, a few works have highlighted the importance of applying multi-level security strategies, targeting device, network, and device layers, to strengthen system resilience. Additionally, several research efforts have justified the need for edge-level processing to ensure low-latency, real-time analysis, especially in time-critical scenarios, which we apply it in this thesis to detect the threat before reach the hospital and take action on real time. In response to these all challenges, this thesis proposes a comprehensive multi-layer security framwork which combines ZTM, IDS, ML, and 2FA at the mobile environment, implemented across the network level and data level.

Chapter 4

Proposed System Architecture and Model

This chapter presents a proposed system design for implementing security in mobile medical systems, with a specific focus on ambulances. The system uses multiple security components: ZTM, 2FA, SIDS, and ML will be used. Both network behavior and data transmission will be analyzed to detect real-time security threats at the edge node that can threaten the system before reaching the hospital, specifically DDoS attacks at the network level and spoofing or injection of patient data, with a specific focus on vital sign.

ZTM: Applies never trust, always verify, so it monitors the behavior of either the network or the transmitted data within the mobile medical system, and upon detecting specific threats, it triggers an isolation mechanism either for the compromised IoMT device or for the ambulance's network interface.

2FA: For user access to IoMT devices in the ambulance (paramedics).

SIDS: To determine the attack threshold at data content level.

ML: Classify data and distinguish between attacks, medical issues, and normal cases.

The following sections present design considerations, the system architecture, components, and proposed model to identify and respond to these threats effectively in real-time:

4.1 Design Considerations

The design of our proposed framework model was done by several considerations, which are:

- **Real-time Response**: The ambulance works in time-sensitive environments, so the system must take the decision rapidly without relying on cloud interaction.
- **Limited Edge Resources**: Due to limited computational capabilities in ambulances or at the IoMT devices themselves, pretrained ML models are deployed to the edge for lightweight real-time inference.
- **Mobile and Unstable Connectivity**: Since ambulances often operate in areas with weak or intermittent internet access, secure authentication and attack detection must occur locally.
- **Sensitivity Data**: Because of sensitivity of patient data, the system must ensure strong protection against both network-level attacks like DDoS and

data-level attacks like injection or spoofing.

- **Behavior-based Monitoring**: As part of the ZTM, the system continuously analyzes both content behavior like abnormal or spoofed patient readings and network traffic like unusual traffic patterns indicating DDoS attacks. This behavior-based analysis is essential for triggering automatic actions such as isolating compromised IoMT devices or the ambulance's network interface, and alerting security before the data reaches the hospital.

4.2 Proposed System Architecture

This section presents proposed system architecture, which consists of three main layers as illustrates in Figure 4.1:

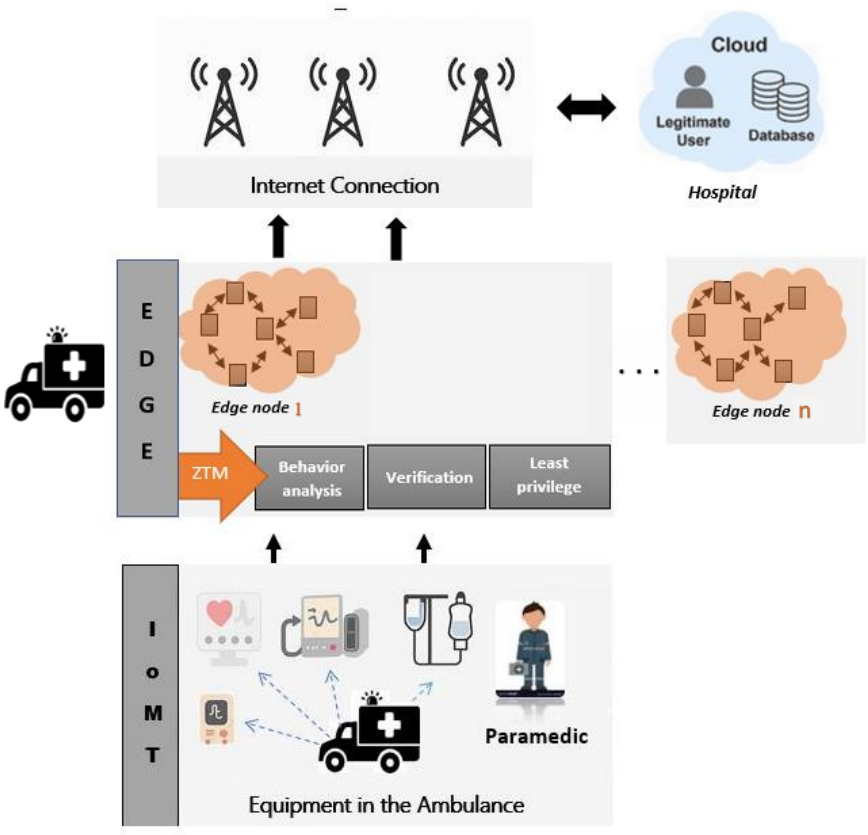

Figure 4.1: Overview of Proposed System Architecture

- Devices: IoMT devices
- Edge nodes: Ambulances, so each ambulance in the system represents an edge node.
- Cloud: Which represents the hospital.

4.3 System Components and Assumptions

This section presents the system components and assumptions for the proposed model. The system components and assumptions are as follows:

(A) Mobile healthcare environment system, which is an ambulance. Each ambulance is modeled as an edge node in the system. The total number of ambulance nodes is represented as shown in Equation (4.1):

$$M = \sum_{i=1}^{n} N_i \tag{4.1}$$

Where:

- M is the total number of ambulance nodes in the system
- N_i is the i-th ambulance node
- n is the total number of ambulances in the system

According to the ZTM principle of being in isolated zones, we **assume** each ambulance operates within an independent network segment. This logical separation facilitates temporary isolation from external communication upon the detection of an attack.

(B) Each ambulance consists of users, which in this case are paramedics, and IoMT devices. We **assume** the paramedics are allowed to use the devices, and they can have read-only access to the medical devices (least privilege according to one of ZTM principle), but they are not trusted by default. They must pass 2FA to access the medical devices inside the ambulance, as shown in Equation (4.2):

$$\text{Access}_{device}(u) = \begin{cases} 1, & \text{if 2FA}(u) = \text{True} \\ 0, & \text{Otherwise} \end{cases} \tag{4.2}$$

Where:

- $\text{Access}_{device}(u)$: Indicates whether the user u is able to access the medical device.
- u: A user attempting to access the device.
- $\text{2FA}(u)$: The result of entering the 2FA for user u.
- 1: The access is accepted.
- 0: The access is denied.

To realize secure access control within the ambulance scenario, we assume that users use a 2FA mechanism that combines biometric authentication like facial recognition with a Personal Identification Number (PIN). Although it's simple, it remains relevant in today's evolving cybersecurity landscape, especially when layered with biometric authentication. The combined approach entails immediate and secure authentication without resorting to external connectivity, and is best suited to the mobile and time-sensitive healthcare environment [48].

Also, the five main IoMT devices are: Heart rate monitor, respiratory rate monitor, temperature sensor, pulse oximeter, and blood pressure monitor. Technical issues may arise with the medical devices used.

(C) We consider the data transmission from the ambulance to the hospitals network to be secure, utilizing trusted security technologies such as encryption.

Specifically, protocols such as Transport Layer Security (TLS) are employed to ensure the confidentiality and integrity of the data while in transit, avoiding any data interception and poisoning attacks. This is because, in previous studies, secure data transmission protocols utilizing symmetric encryption have been successfully applied to ensure the data security of the Internet of Medical Things environment, which protects the data from any kind of attacks during data transmission and storage [78]. However, to avoid any kind of injection attacks, which can be performed at the data source level, we need to consider other types of mitigation techniques. The principle of the ZTM "Never trust, always verify", assumes that channels or connections and devices can be vulnerable to attacks even if they are secured.

(D) Patient data transmission, in this system, refers to the transmission of vital signs collected from the patient in real time under the dataset name Human Vital Sign from the Kaggle site [49]. These vital signs include: Heart Rate (HR), Respiratory Rate (RR), body temperature, Oxygen Saturation (SpO2), Systolic Blood Pressure (SBP), and Diastolic Blood Pressure (DBP).

The description of the dataset from the site taken [49] is:

- Respiratory Rate (RR): considered abnormal if it exceeds 20 breaths per minute or drops below 12.
- Body Temperature: classified as abnormal when it rises above 37.5°C or falls below 36.0°C.

- Oxygen Saturation (SpO_2): marked as abnormal if it is lower than 95%.
- Systolic Blood Pressure (SBP): considered abnormal when it is higher than 140 mmHg or below 110 mmHg.
- Diastolic Blood Pressure (DBP): considered abnormal when it exceeds 90 mmHg or falls below 70 mmHg.

The final classification decision normal or medical issue determined by evaluating all monitored vital signs collectively.

Remaining assumptions:

- It is assumed that the training process was conducted in the cloud due to the limited computational capabilities at the edge, and the trained model is deployed to the edge for real-time inference.
- The devices that may be subject to attacks include the heart rate monitor, respiratory rate monitor, and temperature sensor.
- If an attacker gains access to the specific device, the attacker can propagate to other components, thus affecting decision-making.
- It is assumed that upon detecting an attack coming from a specific IoMT device, the device is temporarily isolated from their network while continuing to operate locally at the ambulance for the paramedics to access its readings, thereby protecting the rest of the system without disabling the device itself.
- The system is assumed to be exposed to two types of attacks:

1. Network-level attacks, such as DDoS attacks.
2. Data-level attacks that involve injecting patient data, either by compromising the device itself or by falsifying the data during its transmission, or due to technical issues existing at the devices.

- Other attacks, either network-level or data-level attacks, can be integrated and implemented in the training model; however, for proof of concept purposes only, DDoS at the network level and injection data level attacks are considered in this work.

4.4 Attack Model

4.4.1 Network-Level Attacks

The attackers are external DDoS networks, as shown in Figure 4.2, and the attacker's goal was to launch a DDoS attack at the network level to disrupt the transmission of vital signs between IoMT devices and the hospital. The success of such an attack can delay or prevent the arrival of critical health data, leading to incorrect or delayed medical decisions. Additionally, the attacker may use this disruption as a distraction to perform other malicious actions, such as injecting falsified data into the system. In some cases, the attack may be carried out with the intent to blackmail the medical institution, threatening further disruption unless certain demands are met. The entry point is an insecure network or unencrypted MQTT messages, and it cannot access the cloud directly [50],[51].

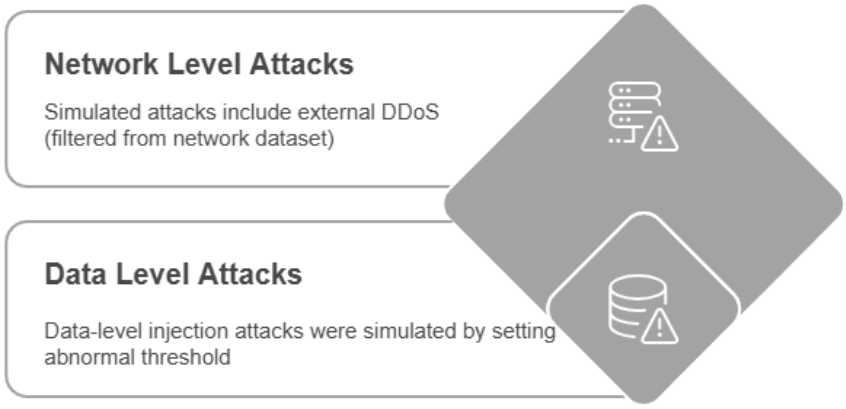

Figure 4.2: Attack Threat in EMS System

DDoS Identification for Enabling Network Isolation

In this thesis, the objective was not to develop a novel classification algorithm for network-level attacks but to distinguish DDoS attacks from other types of attacks at the dataset used using known behavioral characteristics. According to studies [52],[53],[54] and the features exist in the dataset used, inter arrival time which is one of the important feature in DDoS attack is should be short and retain less than one This distinction was necessary to enable network isolation through the ZTM when a DDoS attack is detected. The classification depend on specific traffic features commonly associated with DDoS behavior:

- Extremely short time intervals between packets (frame.time.delta, tcp.tim.delta)
- Use of a specific MQTT message type (mqtt.msgtype = 3)
- Low Quality of Service values (`mqtt.qos` ≤ 1)
- TCP push flag enabled (tcp.flags.push = 1)

- Low values of the MQTT retain flag (`mqtt.retain` ≤ 1)

This classification was applied to records originally labeled as Attack in the dataset, and its purpose was purely functional to support the implementation of network-level isolation without focusing on the classification process itself. The DDoS extraction rules are tuned to the dataset used in this study, so they may vary on different capture types and not generalize to other datasets.

4.4.2 Data Content-Level Attacks:

Because data is valuable, it often becomes a primary target for hackers. As part of the system assumptions, we considered the possibility of data content-level attacks, where an attacker could inject or modify vital sign readings after compromising the device with malicious code to threaten the patient then mislead the medical team by affecting the decision-making [21]. The readings that exceed the maximum thresholds occur only in rare cases, and such increases are accompanied by any abnormal or simultaneous changes in the remaining readings. In the absence of a physiological explanation, this is classified as an attack, such as a body temperature exceeding 43 C and showing logical inconsistency with other vital sign readings, may indicate either device malfunction or malicious data manipulation. To handle this, the proposed system uses predefined medical thresholds to help detect such abnormal values, it used just to generate a simple simulation attacks but ML learn from all vital signs reading. The detailed simulation and how the ML model was trained to recognize these attacks will be explained in Chapter 5. The external attacker's goal is to falsify and distort medical data to mislead medical staff into making incorrect decisions or

re-examining the patient upon arrival, thereby delaying treatment, especially if the intent is to harm the patient. Sometimes, the attacker may have broader objectives, such as blackmailing the institution in exchange for not disrupting the system. The attacker gains access just by compromising device firmware, replacing a legitimate device with a spoofed one, or modifying data during wireless transmission. The success of an attack is measured by checking the data content at the ambulance (edge). If values classified as abnormal exceed the predefined thresholds and absence of a physiological explanation, this indicates that the data have been tampered, and the attacker succeeded in breaching the system.

4.5 ML Workflow and Integration

- The use of ML in this work is justified by the nature of the dataset and the complexity some times of the decision-making process in smart ambulance environments.The vital signs dataset was obtained from Kaggle site [49], where it is clearly described as suitable for training ML models, and it has also been used for ML training in Study [77]. In our work, we added synthetic attack data and 1,500 critical medical issue cases. Due to overlaps between certain cases, as will be explained in the next chapter like a temperature of 45 C reported in Study [79] as a serious medical condition, such values in our study may indicate either device malfunction or an attack or medical issue. Here, ML plays a key role in learning from all available readings and accurately distinguishing between these cases. As for the network dataset on a network level [55], it has also been used in previous studies but only for binary classification, such as Study [56].

Although threshold-based rules can detect simple out-of-range values, they fail to capture multi-IoMT reading correlations (such as temperature, heart rate, respiratory rate, oxygen saturation, and blood pressure), non-linear interactions, and overlapping patterns between Normal, Medical Issue, and Attack states.

- The attacks may originate from one, two, or three devices, creating a multivariate classification problem that cannot be reliably solved using rule-based logic alone. ML allows us to evaluate model performance using different metrics like accuracy, recall and FPR, also compare classifiers such as RF and DT, and identify the best model for the data. It also provides flexibility to expand the system in the future by adding new devices or introducing new attack types

- At the data content level, ML models such as DT, RF, KNN, SVM, and NB were first trained to classify the data into attack, medical issue, or normal. Based on this initial classification, the ZTM-based rule module determined the final action (isolate and alert security, continue transmission, or alert the medical crew) according to trust score calculated.

- At the network level, a rule-based approach was initially applied to generate a classification column with labels such as DDoS, other attacks, and normal traffic as illustrated before, ML models such as DT, RF, KNN, and SVM used to describe the idea as description analysis to aply ZTM in the future work.

4.6 Integrating ZTM

At the data content level we applied ZTM as follows:

- Applying 2FA before the paramedics access the IoMT devices with the least privilege, which means they cannot override the reading.
- Every ambulance (node) in an isolated segment.
- Isolate the IoMT device from which the malicious data come temporally.

4.7 Proposed Model

The proposed model consists of two stages: A training stage in the cloud as illustrates in figure 4.3 and a testing stage at the edge node (ambulance). The proposed system model focuses on integrating multiple security components: ZTM, 2FA, SIDS, and ML to detect threats in real time at the edge node for both the network and data content levels after analyzing their behavior and then taking specific actions.

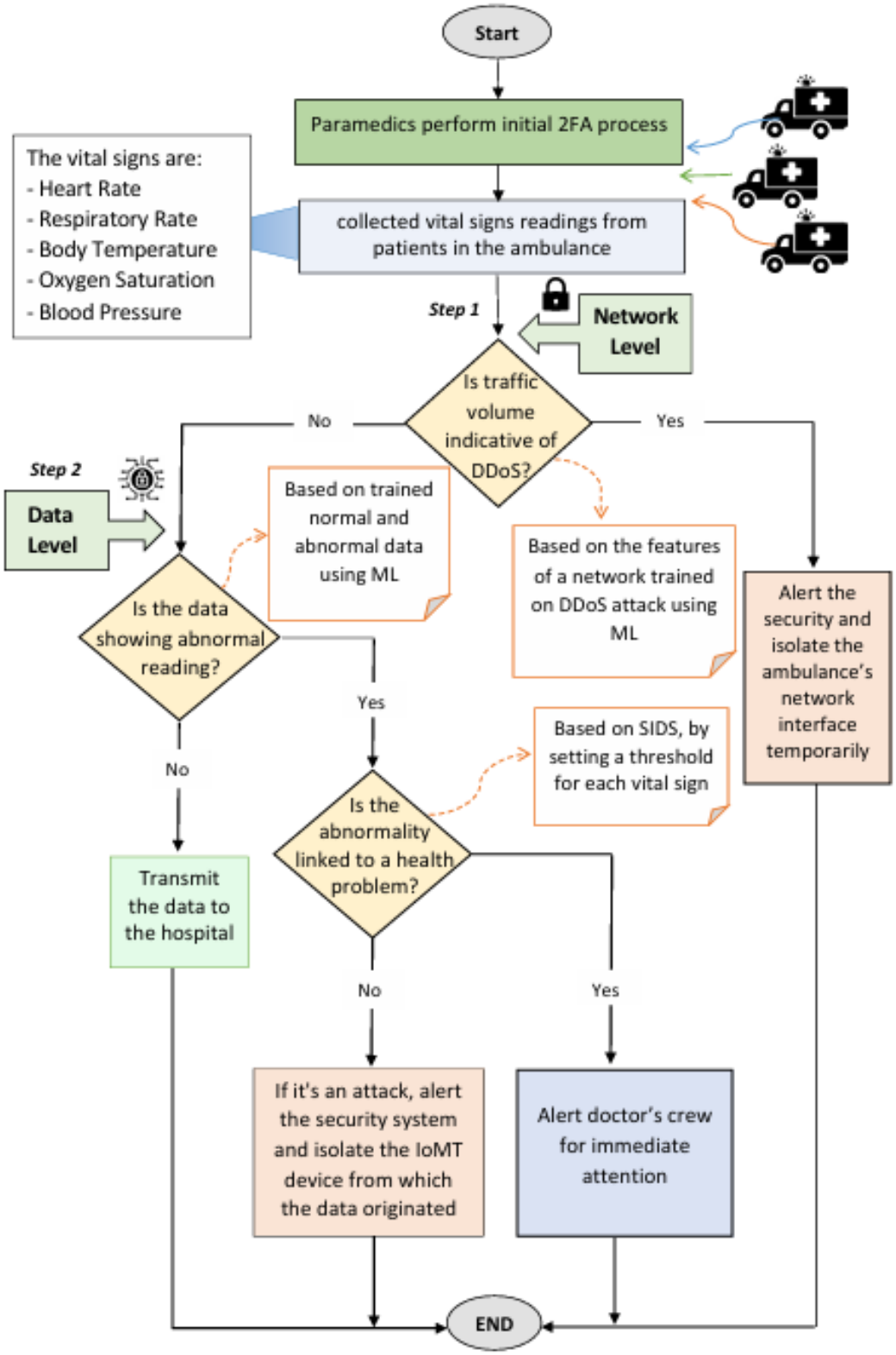

Figure 4.3: Proposed System Model

The vital signs of the patient will be collected at the ambulance by paramedics after performing 2FA to access the devices. The proposed model works on a two-level/step. The first check at the network level is for DDoS attacks; if one is detected, the system will alert security and then isolate the network interface of the ambulance temporarily. If the network is normal, the process moves to check at the second step the data content: distinguish between abnormal due to medical issues or due to an attack, depending on the reading numbers, and take the appropriate action to isolate the compromised device from which the reading comes or alert the medical crew, else at the network level any abnormal activity that does not belong to DDoS is categorized as 'Other attacks' so the system will triger the security.

These steps can be summarized in Algorithm 1 and 2

Algorithm 1 Network-Level After 2FA

```
1: Precondition: Paramedic successfully logged in through 2FA
2: Input: Network traffic features
3: Output: Network status (Normal / DDoS Attack / Other Attack)
4: Apply ML model to classify network traffic
5: if Classification = DDoS Attack then
6:     Alert security team
7:     Isolate external network interface
8: else if Classification = Other Attack then
9:     Alert security team
10: else
11:     Proceed to Data-Level analysis
12: end if
```

Algorithm 2 Data-Content Level with ZTM

Input: Vital signs, ML pred, thresholds, conf_high, conf_medium
Output: isolate device, isolate and alert security team, transit to medical unit, transmit the readings to hospital and monitor
for each patient record **do**
    Compute score_trust = (number of vitals exceeding threshold) / (total number of devices)
    Predict class with ML model → pred
    if pred = "Medical Issue" **then**
        ZTM_Action = transit_to_medical_unit
    else if pred = "Attack" **then**
        if score_trust ≥ conf_high **then**
            ZTM_Action = isolate_device
        else if score_trust ≥ conf_medium **then**
            ZTM_Action = isolate_and_alert ▷ Re-read vitals once before deciding to isolate
        else
            ZTM_Action = alert_security_team
        end if
    else
        ZTM_Action = Transmit the readings to hospital and monitor
    end if
end for

4.7.1 Testing Stage at the Edge

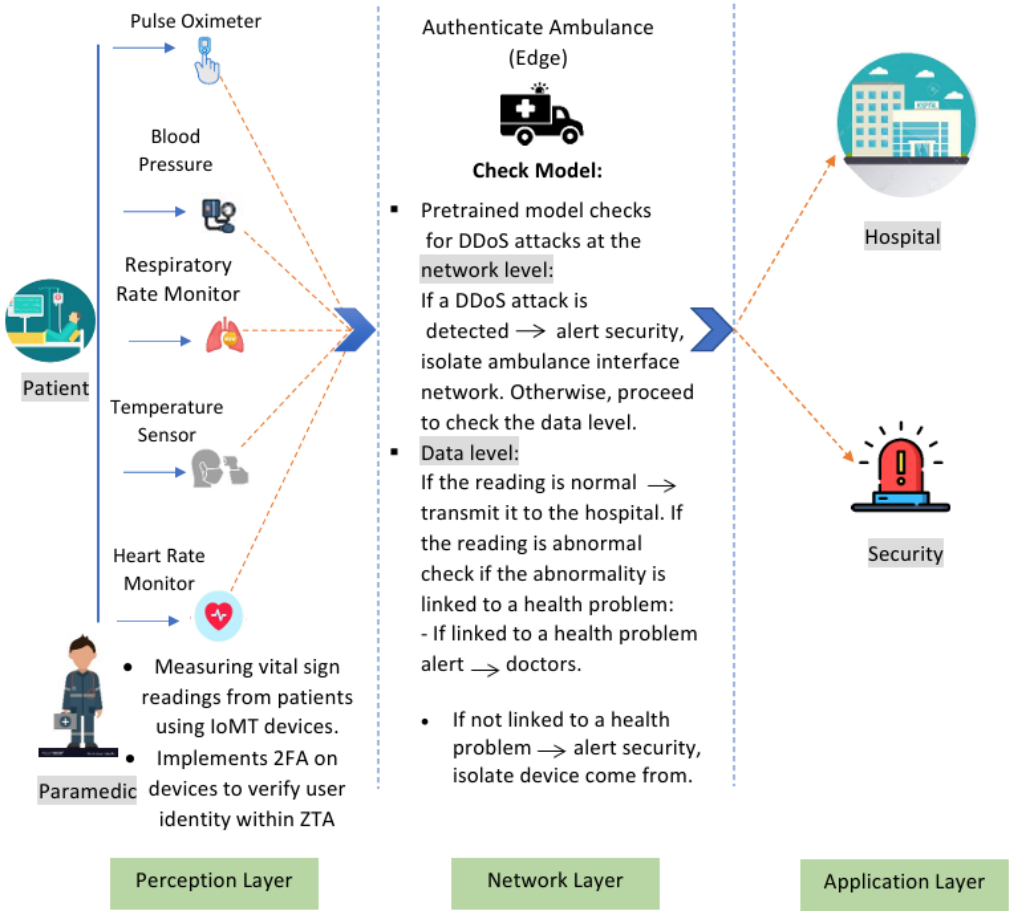

Figure 4.4: Pretrained Security Model Deployed at the Edge for Ambulance System

After training the ML models in the cloud, the trained model will be deployed at the edge, that is mean on all ambulances, to enable real-time decision-making and and then apply response action.

Chapter 5

Security Model Simulation and Results

In this chapter, we will present the simulation used to implement the proposed security model in the EMS system, which builds upon the assumptions and system design that were introduced in chapter 4. The model enhances security through 2FA, detects real-time threats using SIDS and ML, and applies appropriate actions through ZTM. As a result, the system can distinguish between a medical issue, cyberattack and normal in specific cases while ensuring the protection of the patient's health data. The model will be evaluated using performance metrics and will be explained in detail, in addition to comparing the work with previous studies.

5.1 Simulation Environment and Tools

This section discusses the simulation environment and tools that are used to implement the proposed framework model. It covers the hardware and software environment, development tools, and ML and real-time detection support libraries. Datasets, both healthcare network traffic and vital signs, are discussed along with preprocessing steps. Finally, how synthetic attacks are inserted into the data.

5.1.1 Hardware Configuration

The experiments and simulations in this thesis were conducted using a Dell Latitude E6440 laptop. The device is equipped with an Intel® Core™ i7-4600M CPU running at 2.90 GHz, 4 GB of RAM, and a 64-bit Windows 10 Pro operating system (Build 19045). All simulations and implementations were executed under this hardware environment.

5.1.2 Software Tools and Libraries

All simulations, data processing, and machine learning experiments were implemented using the Python programming language (version 3.9). The experiments were conducted using Visual Studio as the primary development environment. The implementation relied on several scientific and machine learning libraries, including NumPy, Pandas, and Matplotlib for data manipulation and visualization; Scikit-learn for building and evaluating classification models.

5.1.3 Dataset Description and Preprocessing

In this thesis, we used two separate datasets: One for the content of the data (vital signs) and the other for the network traffic related to the vital signs. This separation is because, to the best of our knowledge, no publicly available dataset exists that combines both types (vital sign content and its corresponding network traffic). Therefore, we used two distinct but thematically related datasets to simulate and analyze both content-level and network-level behaviors.

Dataset of Vital Sign Readings

- The name of dataset is Human Vital Sign Dataset, from the Kaggle website, 200,000 rows [49].
- The original dataset contains 16 features, including patient identifiers, timestamps, and various vital signs. However, for the purpose of risk classification, only 7 key features were selected based on calculate the correlation between them: heart rate, respiratory rate, body temperature, oxygen saturation, systolic blood pressure, diastolic blood pressure, and derived BMI, which is the difference between height and weight. The simple case senario attack was added to the dataset to simulate an injection attack.
- Figure 5.1 illustrates the preprocessing for the data before starting the training. The dataset used in this study is a supervised learning dataset, where it is labeled as either normal or abnormal based on medical readings, then we added the synthetic data and simple noise percent. The classification was performed using medical values, as detailed in Chapter 4, which considers vital signs such

as heart rate, respiratory rate, temperature, oxygen saturation, blood pressure and BMI.

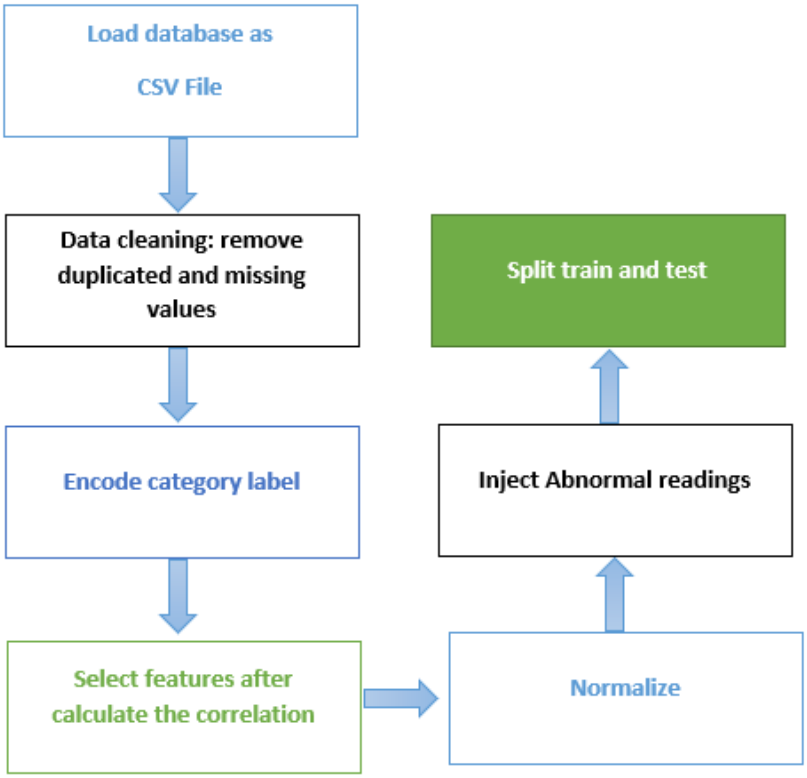

Figure 5.1: Data Preprocssing

5.1.4 Attack Injection Simulation

A simulation attack generation method was used to train the ML model to detect data-level spoofing attacks or injections. We simulated the attacks as the simplest possible scenario to enable us to proceed with the work, since the required dataset was not available to the best of our knowledge. We search for healthcare problems

and spoofed or injected data.

- A total of 81,621 attack instances were synthetically generated.
- Medical issue cases were added to the dataset to increase the overlap with attack instances. Specifically, 1,500 cases of medical issues were incorporated, resulting in a new total dataset of 283,120 records.
- The dataset was split into two parts: 70% was used for training the ML model, and the remaining 30% was reserved for testing. This split is consistent with the partitioning used in most previous studies. Various training/testing ratios were also experimented with, and the 70/30 split was found to yield the best performance for the models in this study.
- This was achieved by injecting randomly generated extreme values that exceed predefined medical thresholds for selected vital signs, including heart rate, respiratory rate, and body temperature, as illustrated in Equation (5.1).
- The thresholds were chosen according to well-known medical ranges for vital signs. For healthy adults, the normal HR is about 60–100 bpm, the normal RR is 12–20 breaths per minute, and normal body temperature is around 36.5–37.3 °C [47]. Readings higher than 150 bpm, 35 breaths per minute, or 43 °C are far above what is normally seen, even in most medical emergencies,exceeding these threshold values may indicate the presence of an injection attack or a technical issue. In rare cases, it could also correspond to an actual medical issue. ML models are employed to distinguish between these scenarios, where

the absence of physiological consistency across all readings serves as a strong indicator of an injection attack.

$$D(i) = \begin{cases} \text{Attack}, & \text{if } ((HR > 150) \ \vee \ (RR > 35) \\ & \quad \vee \ (Temp > 43^{\circ}\text{C})) \ \wedge \ \text{readings are physiologically inconsistent} \\ \text{Medical Issue}, & \text{if } (HR > 100) \ \vee \ (RR > 20) \\ & \quad \vee \ (Temp > 37.3^{\circ}\text{C}) \ \wedge \ \text{readings are physiologically consistent} \\ \text{Normal}, & \text{if } (HR \leq 100) \ \wedge \ (RR \leq 20) \ \wedge \ (Temp \leq 37.3^{\circ}\text{C}) \end{cases} \tag{5.1}$$

Where:

- i – Represents an abnormal case
- $D(i)$ – Decision function that classifies the abnormal case as either an Attack or a Medical Issue.
- HR – Heart Rate (beats per minute)
- RR – Respiratory Rate (breaths per minute)
- $Temp$ – Body Temperature (in Celsius)

This attack is generated to simulate how the system responds to manipulated vital signs. Although some of the injected values may overlap with readings typically associated with medical issues, the remaining vital signs provide enough context for the ML model to distinguish between medical issues and attack scenarios to build

the basic model and then in future integrate other IoMT devices or attacks.

Healthcare Network Traffic Dataset

- The name of dataset is ICU Healthcare Security Dataset, 188,695 rows, with network features [55].
- Includes four attack types: MQTT DDoS, MQTT Publish Flood, Brute Force, and SlowITE.
- It is mainly labeled as normal or attack traffic. Our focus was on DDoS attacks, and we classified the data into three classes: normal, DDoS, and other attacks, as explained before. This label enables network isolation through the ZTM when a DDoS attack is detected.
- The DDoS class is defined based on known characteristics as explained in Chapter 4. This dataset was chosen because it includes network features used in transmitting vital signs, which makes it suitable for the context of this work.

5.2 Simulation Flow

To simulate the proposed model we apply these steps in both the network level and the data level:

1. System Initialization and Authentication
    - Each ambulance consists of paramedics and IoMT devices, and they should implement 2FA to access the medical devices.
    - Collecting vital signs from IoMT devices and sending them to the edge node, then to the hospital (cloud).

- Connections and devices can be vulnerable to attacks even if they are secured according to the ZTM principle: 'Never trust, always verify'. So we examine both the data and the network levels, focusing on two types of attacks and preventing them from causing harm to the patient through the application of temporary isolation.

2. Training and Testing

   At the network dataset: 70% was used for training the ML model and the remaining 30% was reserved for testing according to other study splits. At the data content level: 70% was used to train the ML model and the remaining 30% was reserved for testing after experimenting with multiple split ratios, this configuration achieved the best performance.

3. Machine Learning Models

   ML was used to predict and classify traffic into three categories: attack, normal, and medical issue. at the data content level. The predicted result is then compared with the calculated trust score to verify the patient's condition before taking further action, such as temporary isolation, continuing data transmission, or alerting the medical or security team. Several ML models were evaluated. The best performance was achieved using DT at the network level, and DT, RF, and KNN at the data level.

4. ZTM

   Apply it to isolate a compromised IoMT device from their network or isolate the ambulance network interface after analyzing both the content and the network

behavior.

5. The programming simulation: implemented using the Python language, with several libraries previously mentioned.

6. Response and Logging:

   If no attack is detected, normal data will transmit to the hospital dashboard for medical decision-making. If an attack is detected at data content level, it will compare with the trust score to take the response; the details are logged for forensic analysis.

5.3 Evaluation

Although the proposed system was evaluated through simulation and ML–based detection metrics and memory usage, this approach aligns with current recommendations in the field. According to [4], the IoMV remains a developing area with limited real-world testbeds or standardized evaluation frameworks. The authors emphasize the role of AI-driven techniques in handling cybersecurity threats across network and data layers. Hence, the evaluation strategy in this thesis relies on synthetic data generation and widely used performance metrics, consistent with the evolving methodologies in IoMV research.

5.3.1 Evaluation Environment

Dell Latitude E6440 laptop. The device is equipped with an Intel® Core™ i7-4600M CPU running at 2.90 GHz, 4 GB of RAM, and a 64-bit Windows 10 Pro operating system (Build 19045). All simulations and implementations were executed under this

hardware environment.

5.4 Descriptive Analysis

In this section, we present a descriptive analysis on a two datasets used in the thesis. The focus will be on the vital signs dataset at the data content level. The network dataset, being preprocessed, was reclassified to focus on DDoS attacks and apply the ZTM approach in the future.

5.4.1 Descriptive Analysis of the Network Dataset

- Dataset Overview

  The name of dataset is ICU Healthcare Security Dataset from the Kaggle site [55], with 188,695 records, with 54 network features. Includes four attack types: MQTT DDoS, MQTT Publish Flood, Brute Force, and SlowITE. labeled as normal or attack traffic, we use it because, up to our knowledge, this is the most sutable dataset exist contain network features for the vital signs taken from multiple IoMT devices and has DDoS attacks.

  Feature Selection

  This dataset contains nearly 54 features; however, only 10 were used, following the approach of a previous study [56] after analyzing and selecting the most relevant features which are:

  - frame.time.delta, tcp.time.delta, tcp.flags.ack, tcp.flags.push, tcp.flags.reset, mqtt.hdrflags, mqtt.msgtype, mqtt.qos, mqtt.retain, mqtt.ver.

- Data Preprocessing and Reclassification

  The dataset contains 4 main attacks: DDoS, MQTT Publish Flood, Brute Force, and SlowITE We classified the data into three classes: normal, DDoS, and other attacks to focus only on DDoS according to the general characteristics explained in the previous chapter.

- Analysis of Dataset Charts

  The following Figure 5.2 illustrates the percentage distribution of samples in the dataset at the network level [55]. The dataset was reclassified into three categories, as described on pages 55–56: DDoS, Normal, and Other Attacks.

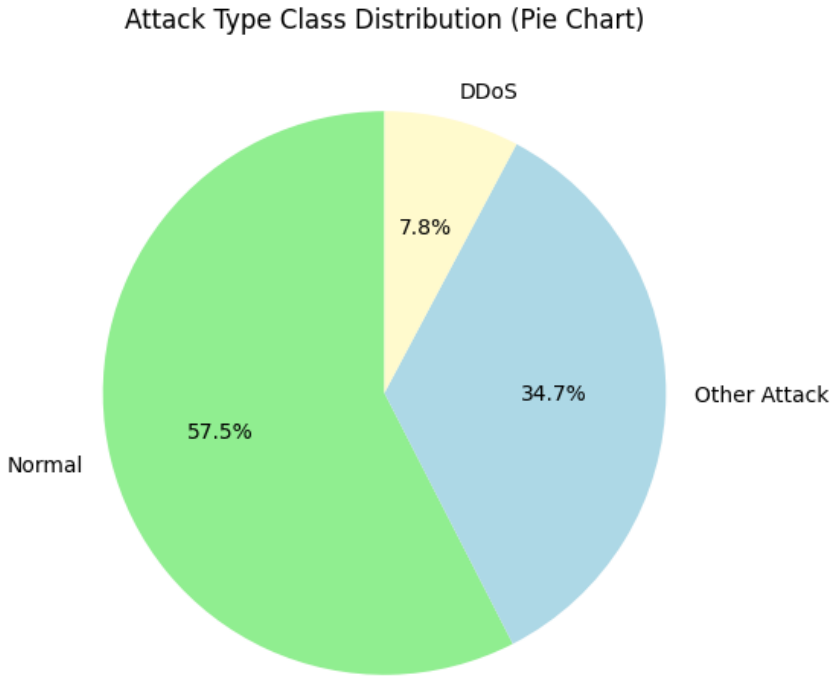

Figure 5.2: Pie Chart of Network Traffic Sample Proportions: Normal, Other Attacks, and DDoS

The pie chart shows the relative proportion of each class. Normal traffic represents the largest share at 57.5% (108,568 samples), followed by other attack types at 34.7% (56,455 samples), while DDoS accounts for approximately 7.8% (14,671 samples). This distribution highlights that healthcare environments are targeted by DDoS attacks, emphasizing the need to focus on detecting and mitigating such threats.

5.4.2 Descriptive Analysis of the Vital Signs Dataset

- Dataset Overview

  The name of the dataset is Human Vital Sign Dataset [49], from the Kaggle website, 200,000 records. Contains 16 features, including patient identifiers, timestamps, and various vital signs. A total of 81,620 attack instances were synthetically generated as described in the previous chapter and 1500 case of medical issues was added to become the new dataset with 283,120 records.

- Data Preprocessing

  During the data preprocessing step, the dataset was cleaned by addressing missing values and removing duplicates. After cleaning, a correlation analysis was performed to explore the relationships between features and assist in selecting the most relevant attributes for modeling, data was split at the patient level, with training and testing sets strictly separated. Features were checked to ensure no overlap with labels or future information, confirming the absence of data leakage.

- Feature Selection

The number of key features was selected based on calculating the correlation between them are: heart rate, respiratory rate, body temperature, oxygen saturation, systolic blood pressure, diastolic blood pressure, and derived BMI, which is the difference between height and weight, and timestamp.

- Analysis of Dataset Chart

  Figure 5.3 illustrates the percentage distribution of each class in the dataset at the data content level. The dataset is divided into three classes: Normal, Medical Issue, and Attack. Based on the original Kaggle dataset [49], the data were modified by adding simple attack scenarios.In order to improve the realism of the dataset and create class overlap between attack and medical issue scenarios, 1,500 additional medical issue samples have been generated based on a clinically documented patient case as reported in literature [79]. Physiological readings from the reference case have been used to synthesize similar data, thus creating diversity and ensuring the robustness of model evaluation under adverse classification conditions. and 1,500 medical issue cases to enhance class representation.

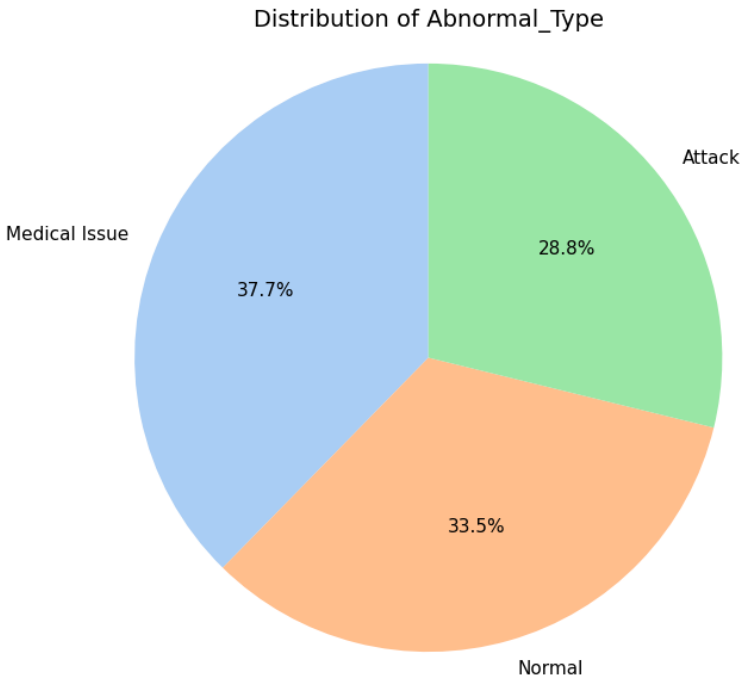

Figure 5.3: Pie Chart of Vital Signs Sample Proportions: Medical Issue, Normal, and Attack

The proportion of attack data added to the original dataset was adjusted to be balanced with the other classes, similar to study [57], which used a dataset in the healthcare system domain where attack data represented 42.5% of the total samples, in order to improve the performance of the machine learning model. Medical issues (37.7%), normal cases (33.5%), and attacks (28.8%). The pie chart illustrates the relative proportion of each class in the dataset, providing an overview of class distribution, highlighting that medical issues

form the largest portion of the dataset, followed by normal cases, while attacks constitute the smallest share.

The Figure 5.4 illustrates the distribution of heart rate and respiratory rate values categorized into normal and abnormal cases. The histograms show the frequency of samples within each vital sign range, with colors representing: green for Normal, blue for Medical Issue, dark red for Attack (This IoMT / Data Injection): Meaning the attack originates from the same IoMT device (HR on the left chart, RR on the right chart), and yellow for Attack from (Other IoMT), indicating an attack targeting another IoMT device (respiratory rate or body temperature on the left chart, and heart rate or body temperature on the right chart).

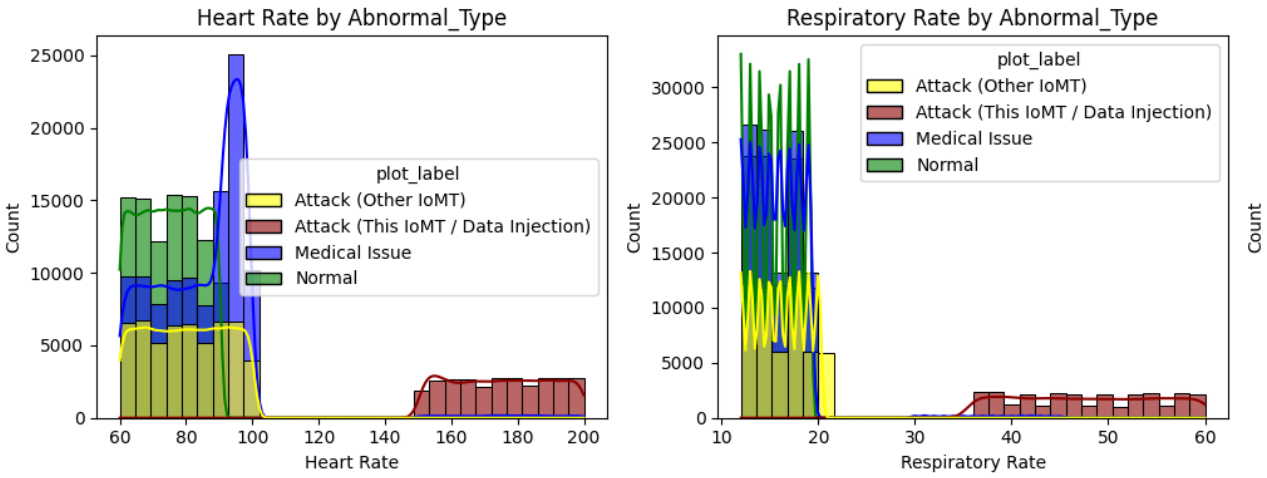

Figure 5.4: Distribution of Heart Rate and Respiratory Rate by normal and abnormal Types, Normal, Medical Issue, and Attack Cases

The Figure 5.5 also illustrates the distribution of body temperature values categorized into normal and abnormal cases. Colors represent: green for Normal, blue for Medical Issue, dark red for Attack (This IoMT / Data Injection) :Meaning the attack originates from the same IoMT device measuring body temperature, and yellow for Attack (Other IoMT), indicating an attack targeting another IoMT device such as heart rate or respiratory rate. So this is why we use ML, because the abnormality is due to many reasons, and we need to analyze it.

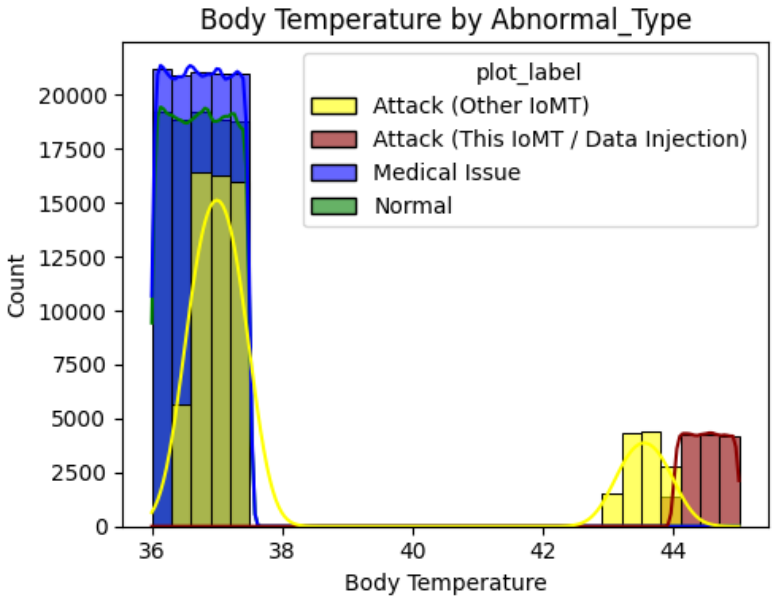

Figure 5.5: Distribution of Body Temperature by Normal and Abnormal Type, Normal, Medical issue, and Attack Cases

5.5 Performance of ML Classifier

Because we work on two-levels analysis as described before the performance will be in a two stage, the first at the network level and the second on a data content level with foucus on data content. The proposed model was evaluated using overall accuracy, Recall, Precision, F1-score, False Positive, False Negative, Training Time, and Testing Time, and Memory Usage.

5.5.1 The Performance Metrics used

The evaluation of the proposed ML model aligns with the current recommendation in study [4], which will be conducted on two levels. At the network level, the focus will be on assessing the efficiency of ML models in classifying the case at the 2 levels. The appropriate action under the ZTM, including isolating the network interface of the ambulance, checking data content, and alerting security. At the data content level, the evaluation will proceed in two stages: First, testing the classification of vital signs and abnormal patterns and comparing the overall accuracy of ML models to find the best model and second after integrating ZTM with ML predict result after classifiying to take the propriate next action comparative with ZTM. The following standard metrics were used a macro average for: **Accuracy**, **Precision**, **Recall**, **F1-score**, and **FPR**, **FNR** for each class, **ROC-AUC**, **MCC**, **Cohen's Kappa**, **Time detection**, and **Memory usage**.

- Accuracy: Represents the overall proportion of correctly classified instances among all tested cases [67], defined as the following Equation 5.2

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{5.2}$$

Where:

TP = True Positives.

TN = True Negatives.

FP = False Positives.

FN = False Negatives.

- Macro averaged precision, recall, F1-score.

  - Precision [66]: It measures the reliability of positive predictions. Calculate number of True Positives TP , False Positives FP, and False Negatives FN for each class then calculate then calculate the precision as illustrated in Equation 5.3

$$\text{Precision} = \frac{TP}{TP + FP} \tag{5.3}$$

Where:

TP = True Positives.

FP = False Positives.

- Average precision [66] then calculated as illustrated in Equation 5.4

$$\text{Precision}_{\text{macro}} = \frac{\text{Precision}_{\text{class A}} + \text{Precision}_{\text{class B}} + \cdots + \text{Precision}_{\text{class N}}}{N} \tag{5.4}$$

Where:

N = Number of classes.

- Recall: It measures the ability of the model to correctly identify all actual positive cases [67].

$$\text{Recall} = \frac{TP}{TP + FN} \tag{5.5}$$

Where:

TP = True Positives.

FN = False Negatives.

- Average recall [66] then calculated in Equation 5.6

$$\text{Recall}_{\text{macro}} = \frac{\text{Recall}_{\text{class A}} + \text{Recall}_{\text{class B}} + \cdots + \text{Recall}_{\text{class N}}}{N} \tag{5.6}$$

- F1-score [67]: is the harmonic mean of Precision and Recall, providing a single metric that balances the trade-off between false positives and false negatives.

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5.7}$$

- Averaged F1 [65] is calculated by first computing the F1 score for each class, then taking the simple (arithmetic) average of these scores as illustrates in Equation Equation 5.8

$$F1_{\text{macro}} = \frac{1}{N} \sum_{i=1}^{N} F1_i = \frac{1}{N} \sum_{i=1}^{N} \frac{2P_i R_i}{P_i + R_i} \tag{5.8}$$

Where:

- N: Number of classes.
- $F1_i$: F1-score of class i.
- P_i: Precision of class i.
- R_i: Recall of class i.

- False False Positive rate (FPR) identifies the proportion of negatives classified as positive. Minimizing FPR is important to avoid false alarms in emergency systems [67].

$$\text{FPR} = \frac{FP}{FP + TN} \tag{5.9}$$

Where:

FP = False Positives.

TN = True Negatives.

- FNR a correctly predicted negative outcome [68]. In healthcare and cyber-attack detection, a low FNR is critical to ensure that no critical events are missed.

$$\text{FNR} = \frac{FN}{FN + TP} \tag{5.10}$$

Where:

FN = False Negatives.

TP = True Positives.

- Cohen's Kappa: It measures the agreement between the predictions made by the classifier and true labels, after adjusting for the element of chance that may exist in the data. It performs particularly well on imbalanced data sets. Cohen's Kappa is equal to one when there is a full agreement, zero when it is random, and - 1 when there is a full disagreement [67].

- Matthews' correlation coefficient(MCC): MCC measures the correlation between true and predicted labels, with +1 for perfect, 0 for random, and - 1 for completely wrong predictions [69].

- ROC AUC (OVR): To apply ROC curves and ROC AUC to multiclass prob-

lems, OvR (One vs Rest) is used; one class is treated as positive and all other classes are as negative. This converts the multiclass problem into a binary , allowing the use of standard binary metrics [70].

- Memory Usage: Is the amount of memory space taken up by a system or a program, and it is a key measure to study the efficiency of algorithms. Because the main concern in the EMS environment is the real-time implementation of ML models at the edge, therefore, memory usage was measured during the testing phase to evaluate the feasibility of deploying the models on edge devices.

5.5.2 The Performance Results

5.5.3 Network Level

In this subsection, the performance analysis could be applied after reclassifyed the dataset to highlight DDoS attacks, and applying ZTM depends on the trust score calculated to take the next suitable action to isolate the network interface of the ambulance in the EMS system temporarily as a descriptive idea after an attack is detected. The focus will be on the vital signs dataset, as the network dataset was already prepared and only reclassified to highlight DDoS attacks and apply the ZTM approach after an attack is detected. Figure 5.6 illustrates the overall accuracy comparison of ML model's in predicting the case into DDoS, Normal, and Other attack.Since DDoS instances represent only 7.8% of the dataset, the classes are imbalanced; therefore, additional evaluation metrics are required.

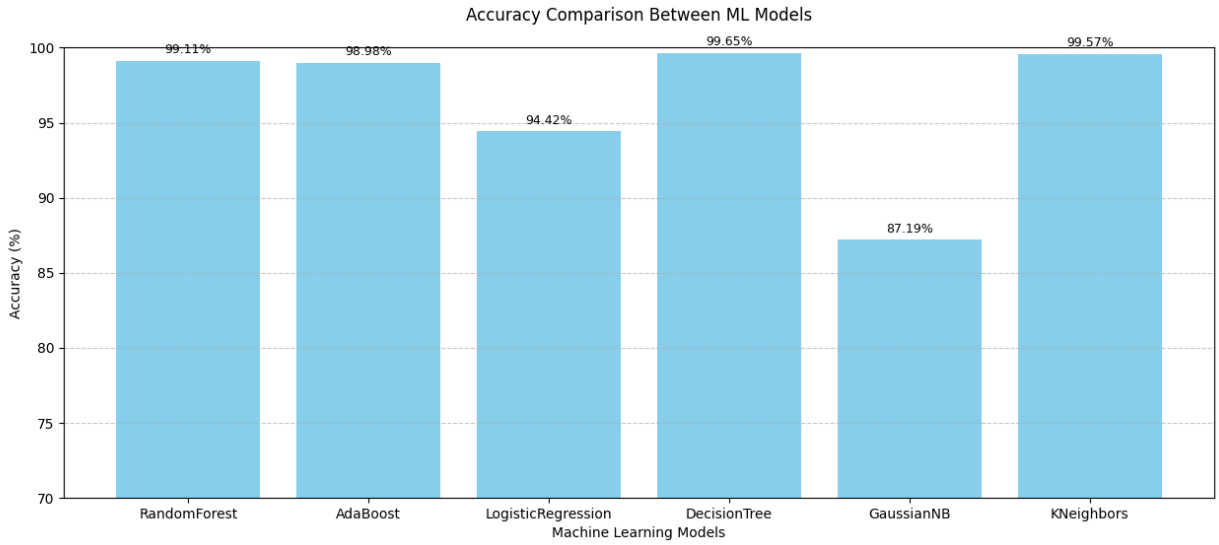

Figure 5.6: Overall accuracy comparison of ML models in predicting the case into DDoS, Normal, and Other attack

The highest accuracy was achieved by DT(99.64%), followed by KNeighbors (99.57%), RF(99.11%), AdaBoost, Logistic Regression (LR), and GaussianNB.

That means we will depend on these three models when applying ZTM to apply the actions in extended experement or future work, including isolating the network interface, checking data content, alerting security upon detecting other attacks, and continuing data transmission.

The following Table 5.1 presents the best performance of different ML models using macro-averaged accuracy, precision recall, F1-score,

Table 5.1: Performance comparison of different machine learning models

Model	Accuracy	Precision	Recall	F1-score
DT	99.64	99.77	99.68	99.73
KNN	99.57	99.64	99.60	99.62
RF	99.11	99.17	98.52	98.84
AdaBoost	98.98	99.26	98.44	98.84
LR	94.41	93.51	94.96	94.09
NB	87.19	93.47	87.79	88.99

The FPR and FNR were computed for each class to analyze false positives and false negatives in the multi-class setting, while the F1-score was calculated as it reflects the balance between precision and recall, these metrics were computed at the optimal configuration for each DT, RF and KNN ML models as illustrated in Tables 5.2, 5.3, and 5.4.

Table 5.2: FPR, FNR and F1- Score per each class in DT machine learning model

Class	F1-score	FPR	FNR
DDoS Attack Class	99.94	0.00007	0.00114
Normal Class	99.7	0.00588	0.00166
Other Attacks Class	99.5	0.00157	0.00713

Table 5.3: FPR, FNR and F1- Score per each class in RF machine learning model

Class	F1-score	FPR	FNR
DDoS Attack Class	98.35	0.00046	0.02719
Normal Class	99.45	0.01019	0.00351
Other Attacks Class	98.73	0.0063	0.01361

The results obtained confirmed that the DT model has the highest classification level effectiveness with the highest F1-scores and lowest FPR and FNR values com-

Table 5.4: FPR, FNR and F1- Score per each class in KNN machine learning model

Class	F1-score	FPR	FNR
DDoS Attack Class	99.84	0.00015	0.00137
Normal Class	99.64	0.00646	0.00234
Other Attacks Class	99.38	0.0022	0.00825

pared to other classes. For example, in terms of dealing with DDoS attack classes, DT clearly fares better than other models. Moreover, in terms of error rate, KNN model results are slightly higher than DT, RF model has higher values in terms of FNR.

ROC AUC (OVR)

The ROC AUC (OVR) scores are good for all three models: DT 99.97%, RF 99.96%, and KNN 99.95% in multi-class. So we also used other metrics like MCC and Kappa to better evaluate the models, especially for any class imbalances.

Cohen's Kappa and MCC

The three models perform very well. For DT, MCC is 99.3% and Kappa is 99.34%; for RF, MCC and Kappa are 98.3%; and for KNN, MCC and Kappa are 99.2%. Along with the high ROC AUC scores, these metrics give a clearer view of how the models handle classes.

Time Detection

Detection time refers to the time required by ML models to identify an event, which in this dataset corresponds to one of three classes: DDoS attack, Normal, or Other

attack. Figure 5.7 illustrates the detection time which achieved by different ML models. Among the evaluated models, Logistic Regression and DT achieved the fastest detection time of 0.0156 s, while KNN required the longest time, 8.7418 s because it is a lazy learning algorithm that computes distances to all training samples for each new instance

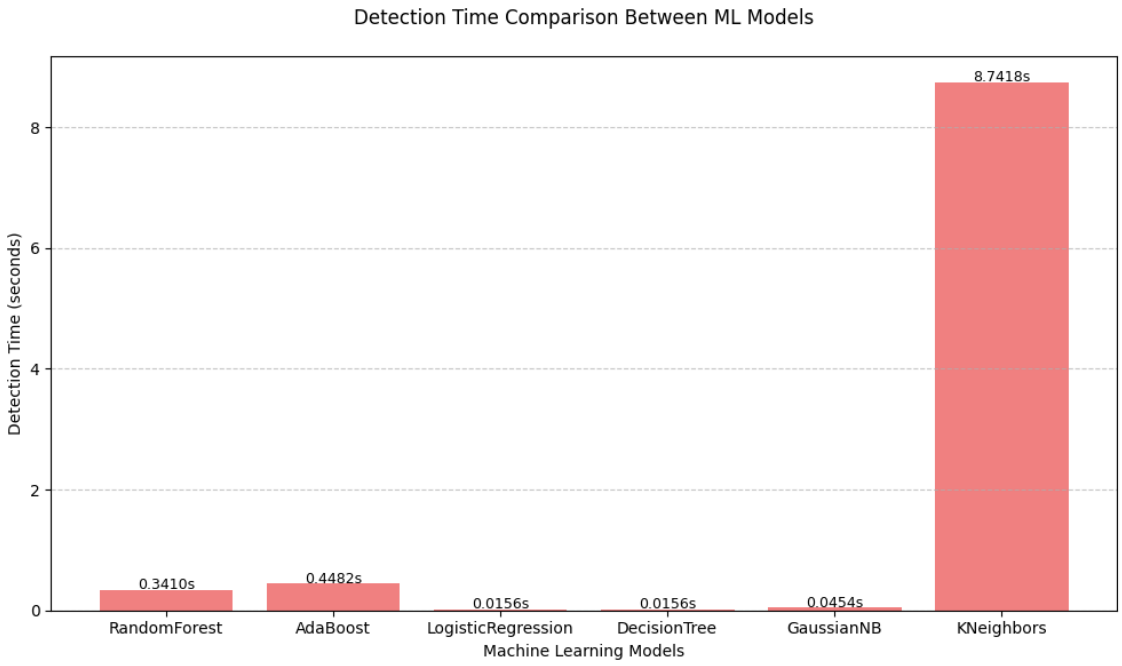

Figure 5.7: Detection Time Required by Different ML Models for Classifying Events (DDoS, Normal, Other attack)

Summary

The system's performance was initially evaluated at the network level, with a particular focus on DDoS attacks. Subsequently, the ZTM was applied, and the system's accuracy in making appropriate decisions based on network analysis was assessed. The DT model achieved the highest accuracy 99.64 %, For the network-level evalu-

ation before applying the action.

5.5.4 Data Content Level (Vital Signs)

This section focuses on the data content level, given its importance and sensitivity. The target column was generated using a rule-based approach to establish a ground truth, based on the vital sign thresholds described in the previous chapter, then used as input to the machine learning models to train the models and simulate accuracy, and evaluate the system's performance and efficiency.

Performance Measures

The following Figure 5.8 illustrates the best overall accuracy achieved to classify each case as: Normal, Attack, and Medical issues after balancing each model.

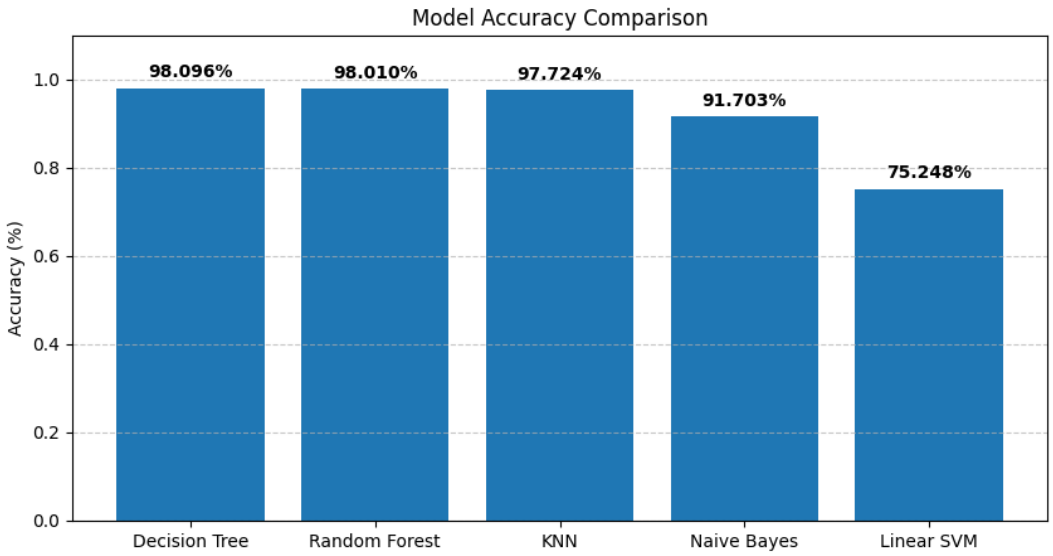

Figure 5.8: The Best Classification overall Accuracy was Achieved for the three Cases (Normal, Attack, and Medical Issues) Using Multiple ML Models

The best three models overall accuracy achieved: Decision Tree 98.096%, followed Random Forest 98.01% and KNN 97.724%. The Naïve Bayes model achieved 91.703%, while the Linear SVM performed relatively lower with 75.248% accuracy.

Model Parameters Adjustment

To achieve these results, the hyperparameters of the top three performing models were fine-tuned and balanced as follows:

- **Decision Tree**

  In this model, different values of the parameters Max Depth and Random State were tested as shown in table 5.5 to determine the best reading. The best accuracy was achieved at a depth of 5, reaching 98.096%.

Table 5.5: Decision Tree parameter settings and macro-accuracy results

Max Depth	Random State	Accuracy(%)	Precision	Recall	F1-score
2	20	61.021	48.74	57.67	49.21
3	50	89.081	90.526	87.506	87.559
4	50	89.54	89.60	89.50	89.55
5	70	98.095	98.385	97.803	98.039
5	100	98.096	98.386	97.804	98.040
5	120	98.095	98.385	97.803	98.039
5	130	98.095	98.385	97.803	98.039
5	140	98.095	98.385	97.803	98.039
5	150	98.096	98.386	97.804	98.040
5	170	98.095	98.385	97.803	98.039

The FPR and FNR were computed for each class to analyze false positives and

false negatives in the multi-class setting, while the F1-score was calculated as it reflects the balance between precision and recall, these metrics were computed at the optimal configuration with max depth = 5 and random state = 100, where the model achieved an accuracy of 98.096% as shown in table 5.6.

Table 5.6: Performance Metrics per Class

Class	F1-score	FPR	FNR
Attack Class	96.543	0.00026	0.06532
Medical Issue Class	97.5	0.03020	0.00056
Normal Class	99.996	0.00004	0.00002

The results indicate strong classification performance across all classes, with particularly low false positive and false negative rates, demonstrating the robustness of the model in the multi-class setting.

- **Random Forest**

  In the RF model, different parameter values were tested to get best performance as illustrated in table 5.7. The main parameters adjusted were: Maximum depth, the number of trees $n_estimators$, and the random state. After experimentation, the best readings were obtained with $(max\_depth) = 3$, $(n\_estimators) = 40$, and the $(random\_state) = 35$, achieving an accuracy of 98.010%. These results demonstrate that a relatively shallow depth with a moderate number of estimators is good for achieving high performance. The detailed parameter settings and outcomes are summarized in Chapter 2.

Table 5.7: Random Forest parameter settings and macro-accuracy results

max_depth	n_estimators	random_state	Acc (%)	Precision	Recall	F1-score
2	20	35	77.966	86.397	80.489	83.6
3	18	35	90.474	92.441	91.564	90.964
3	20	35	90.559	92.537	91.639	91.062
3	25	35	90.532	92.507	91.617	91.03
3	30	35	97.869	97.936	98.112	97.973
3	40	35	98.010	98.093	98.238	98.119
3	50	35	97.986	98.068	98.216	98.094
4	20	35	95.670	96.18	96.165	95.94
4	21	35	90.791	92.804	91.846	91.328

Class-wise F1-score, FPR, and FNR were reported under the optimal configuration with max depth = 3, n-estimators = 40, and random state = 35 where the model achieved an accuracy of 98.01% as shown in table 5.8.

Table 5.8: Performance Metrics per Class

Class	F1-score	FPR	FNR
Attack Class	99.73	0.00210	0.0004
Medical Issue Class	97.287	0.0008	0.0527
Normal Class	97.33	0.0276	0.00011

Although the DT model achieved a higher overall accuracy of 98.096% compared to the RF model's 98.01%, the ensemble approach demonstrates competitive F1-scores and generally lower FPR and FNR across most classes, indicating a more balanced performance in handling FPR and FNR in the multi-class scenario.

- **K-Nearest Neighbors**

  The table 5.9 shows the performance results of the KNN model depending on the choice of $k_neighbors$ While K =7 achieved high overall accuracy 97.724%. Increasing the K value may oversmooth the decision boundary, reducing the model's sensitivity to local patterns and increasing bias (underfitting), so we limited to a maximum of 7.

Table 5.9: Impact of varying $n\_neighbors$ on the performance of the KNN model

$K\_neighbors$	**Accuracy**	**Precision**	**Recall**	**F1-score**
1	92.069	92.142	92.273	92.202
2	91.782	92.166	92.043	91.821
3	96.328	96.375	96.546	96.454
4	96.819	97.043	96.941	96.971
5	97.369	97.497	97.535	97.516
6	97.535	97.711	97.649	97.675
7	97.724	97.849	97.875	97.861

For each class F1-score, FPR, and FNR were reported under the optimal configuration with K = 7 where the model achieved an accuracy of 97.724% as shown in table 5.10.

Table 5.10: Performance Metrics per Class

Class	**F1-score**	**FPR**	**FNR**
Attack Class	99.90	0.0001	0.00004
Medical Issue Class	96.97	0.01618	0.03352
Normal Class	96.62	0.01895	0.03021

KNN achieves good F1-scores, particularly for the Attack class, its FPR and FNR values are generally higher for the Medical Issue and Normal classes

compared to the DT and RF models, indicating slightly less robust handling of false positives and false negatives in the multi-class scenario.

Note: To evaluate the stability of the models and to confirm the reliability of the results, we performed 5-Fold Cross-Validation on the data in the training sets. The following Figure 5.9 compares the test set accuracy of each model with its cross-validation accuracy, reflects a more robust performance estimation, indicating acceptable generalization and minimal overfitting.

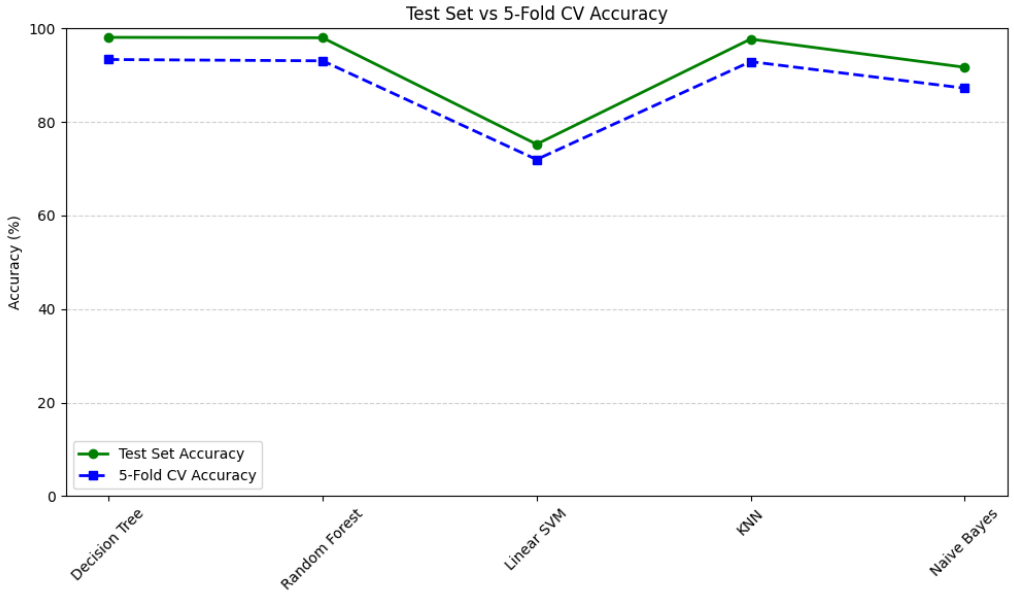

Figure 5.9: Comparison of Test Set Accuracy and 5-Fold Cross-Validation Accuracy for all ML models

ROC AUC (OVR)

At the data level, ROC AUC (OVR) AUC is very good for all models: 99.7% for DT, 99.9% for RF, and 99.82% for KNN. This shows that the models can predict

the classes accurately.

Cohen's Kappa and MCC

At the data level, the models show strong performance. DT, MCC is 97.17% and Cohen's Kappa is 97.12%; for RF, MCC is 97.055% and Cohen's Kappa is 97.002%; and for KNN, both MCC and Cohen's Kappa are 96.56%. These metrics, together with ROC AUC, give a clear view of how well the models capture the relationships between classes.

Detection Time

The detection time is considered one of the most important evaluation criteria in this study, as it has been established as a key standard based on previous studies, as explained. Considering the relatively lightweight models used and the dataset size (281,620 records with a limited number of features), the training and detection times remained low and showed only slight variations between the models, which is reasonable and consistent with the efficiency of such models. The following Figure 5.10 illustrates a comparison between multiple machine learning models in terms of accuracy and detection time (seconds).

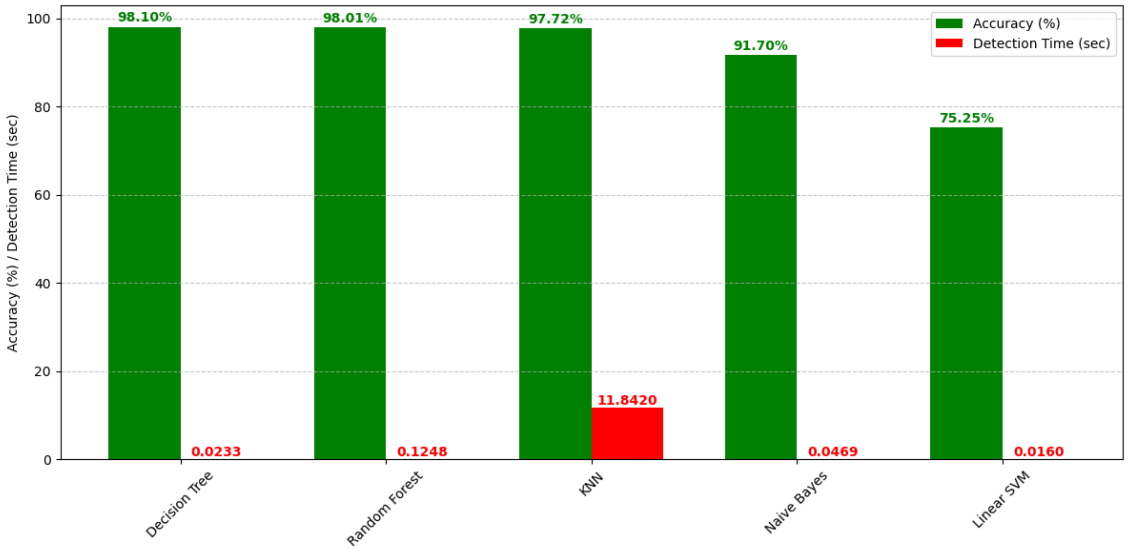

Figure 5.10: Comparison of Detection Time Across Various ML Models

The green bars represent the model's accuracy, and the red bars represent the detection time:

- DT: Achieved an accuracy of 98.10% with the little detection time 0.0233 second.
- RF: Showed 98.01% accuracy but required more time 0.1248 second.
- KNN: Achieved accuracy 97.72% but consumed the highest detection time 11.842 second, making it less efficient for real-time.
- NB: Achieved 91.7% accuracy with a moderate detection time 0.0469 second.

DT demonstrated the best balance between high accuracy and low detection time, making it the most suitable model for real-time detection scenarios. However, al-

though KNN required more processing time.

Memory Usage

At the network level, memory usage was measured while applying ZTM to isolate the ambulance's network interface. At the data level, memory usage was also evaluated when applying ZTM to isolate a compromised IoMT device.

Memory usage was measured while applying the model (test) on the edge node; it means the memory usage while applying the classification. Table 5.11 shows the evaluation at data content level. DT and RF consumed the least resources, making them the most suitable for real-time deployment in resource-constrained EMS environments.

Table 5.11: The memory usage of different ML models at the Data content Level

ML model	Memory Usage (MB)
DT	6.48
RF	6.94
KNN	23.84
NB	13.89

5.5.5 Performance Evaluation and Results of Applying ZTM at Data Content

The performance of the ZTM in this work is evaluated after the integrated ML model result is predicted with the trust score calculated as explained in Ch4 according to

the principle 'Never trust, always verify' before taking the appropriate action, like isolating the compromised device, alerting security, or continue transmit the data to the hospital.

Performance Measure

After training deferent ML models on a dataset used specially at data content level (vital signs) which has three cases: attack, medical issue, and normal we compare the predicted result with the calculated trust score for each row for nearly 85,000 samples to provide astaticly representative performance results to reduce the FPR in decision-making. Table below 5.12 demonstrates the accuracy, FPR, execuion time, and memory usage of decision-making after integrate the results of each ML model with ZTM.

Table 5.12: ZTM-Integrated ML Model Performance Comparison

ML Model	Acc	FPR	Execution Time (sec)	Memory Usage (MB)
DT	98.096	0.00008	5.9677	41.594
RF	98.01	0.00094	9.854	44.887
KNN	97.73	0.00002	13.7	53.121

- **DT classifier:** The integration of the ZTM with the DT classifier achieved a decision accuracy of 98.01%, with an almost negligible FPR of 0.00008. The overall accuracy remained unchanged because the DT at depth 5 had already achieved a very low FPR. To evaluate the effect of ZTM further, we applied it

to DT models trained at different depths, as illustrated in Figure 5.11.

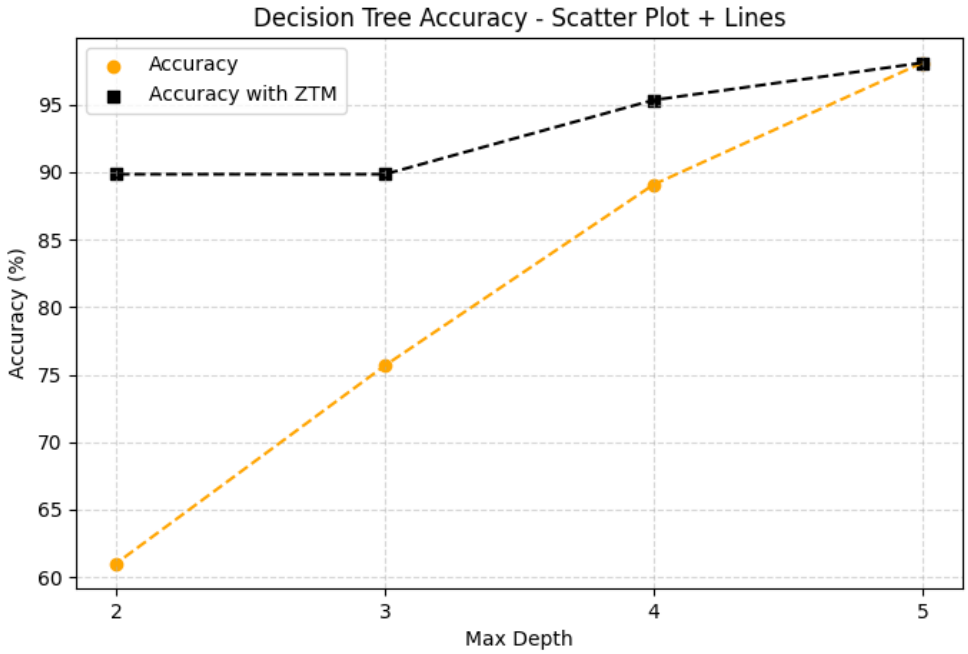

Figure 5.11: Performance Comparison of the Decision Tree Classifier at Different Depths after Integrating ZTM

As illustrated, integrating ZTM significantly improved the DT classifier's performance: at depth 2, accuracy increased from 61.02% to 89.84%, while at depth 4, it rose from 89.08% to 95.34%.

- **RF classifier:**Integrating the ZTM with the RF classifier achieved a decision accuracy of 98.01% with a low FPR of 0.00094. Since the FPR was already very small, the effect of ZTM on this model was not clearly observable. Therefore, we evaluated the impact of ZTM by training RF models with different numbers of estimators and depths. The differences were minimal; for instance, at depth

2 with 20 estimators, the accuracy increased slightly from 77.97% to 77.99%.

- **KNN classifier:**Integrating this ML model with the ZTM resulted in a slight increase in accuracy, from 97.72% to 97.73%, with a nearly zero FPR of 0.00002. This highlights the role of ZTM in enhancing the model's reliability, even when the improvement in accuracy is minimal. Figure 5.12 ilustrates these results.

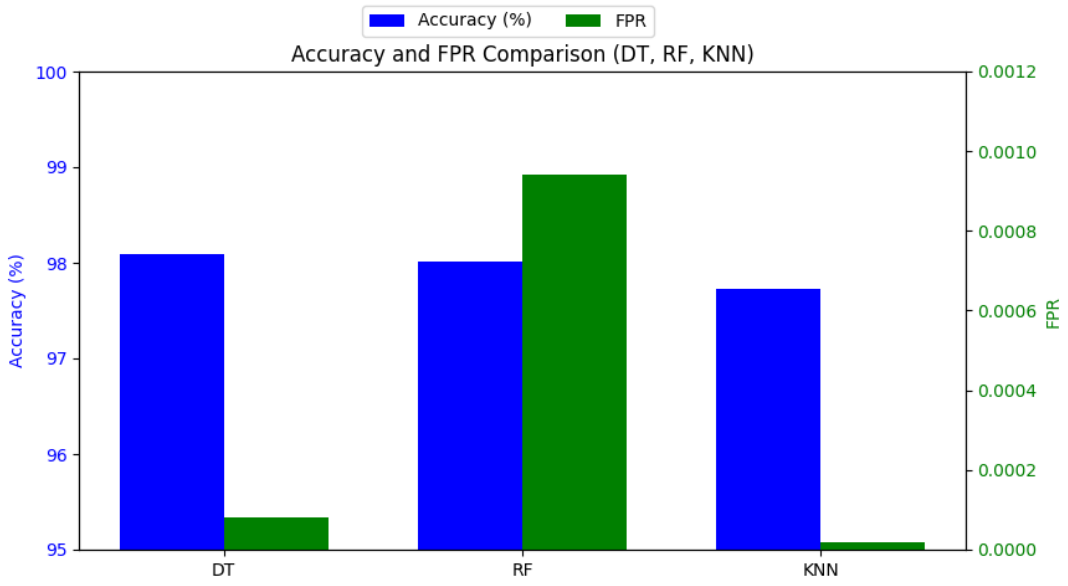

Figure 5.12: Performance comparison after integrating ZTM with ML classifiers, demonstrating enhanced decision accuracy and lower FPR

So applying ZTM improved security decisions over the original ML model by integrating trust levels in isolation and response.

5.5.6 Extended Experiment: Integrating the "Trust" Feature in Training the ML Models

To study the impact of introducing ZTM during the model training and simulation process, an additional experiment that included a new feature, Trust, was conducted. This feature was assigned a value of 1 if any vital sign reading exceeded the predefined threshold and 0 otherwise, as illustrated in the Algorithm 3 below. Then, this feature was included in the training of ML models as explained in Chapter 5, to assess its impact on model performance.

Algorithm 3 Compute Trust Feature for Each Row

Input: Vital Signs reading
Thresholds:
    Heart Rate > 150
    Respiratory Rate > 35
    Body Temperature > 43
Output: Dataset with new column `Trust`
for each row in Dataset **do**
    `count` ← 0
    if row['Heart Rate'] > 150 **then** `count` ← `count` + 1
    end if
    if row['Respiratory Rate'] > 35 **then** `count` ← `count` + 1
    end if
    if row['Body Temperature'] > 43 **then** `count` ← `count` + 1
    end if
    `trust` ← `count` ▷ 0 if none, 1-3 otherwise
    Add `trust` to current row
end for

The results were as follows:

- The results showed that the performance did not change for KNN and SVM in view of the fact that they showed identical results before and after adding

the Trust feature.

- The improvement was observed in the RF and DT models:

  - RF model: The accuracy improved significantly for lower numbers of estimators and maximum depths up to 3, as illustrated in Figure 5.13. Prior to adding the Trust feature, the model achieved accuracies ranging from 90.42% to 90.55% for 10–14 estimators. After including the Trust feature, the accuracy increased substantially, reaching 98.01% to 99.88% at 40 estimators.

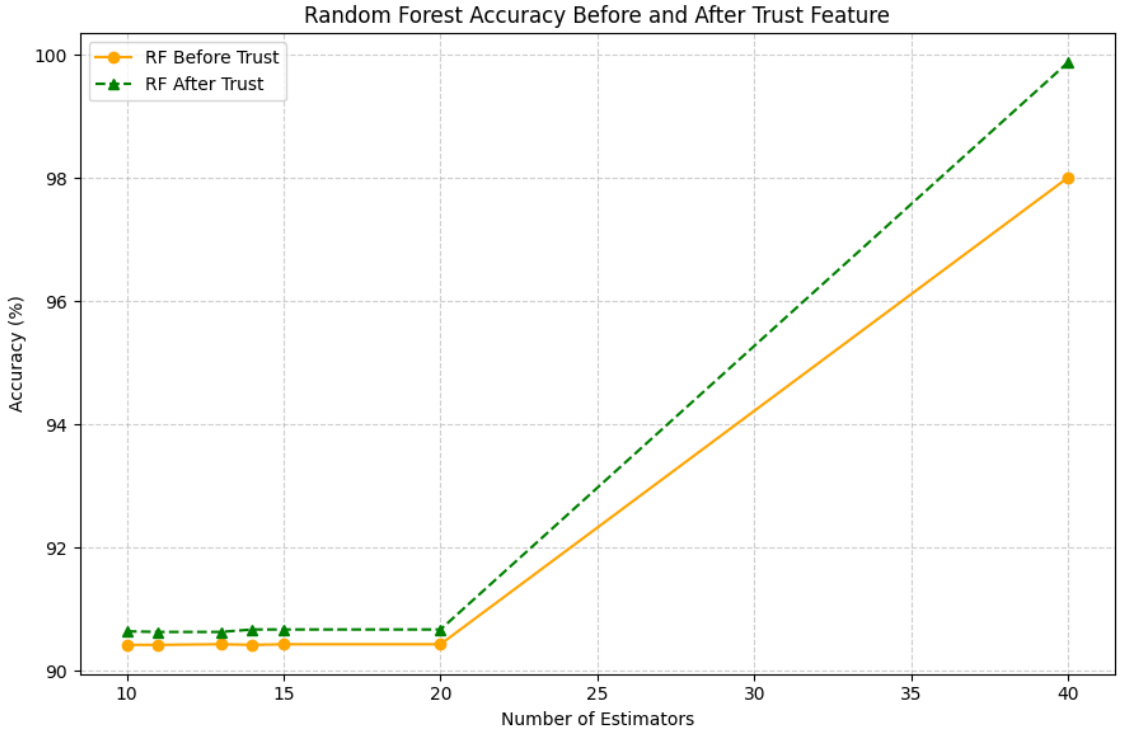

Figure 5.13: Performance Comparison of the RF Model Before and After Adding the Trust Feature

  - For the Decision Tree (DT), when the maximum depth was set to 3, the accu-

racy increased from 75.67% to 90.79% with the addition of the Trust feature. At higher depths of 4 and 5, the accuracy further improved after including the Trust feature, reaching 98.096%, as illustrated in Figure 5.14, thereby surpassing the previous results and approaching near-perfect performance.

Figure 5.14: Performance Comparison of the DT Model Before and After Adding the Trust Feature

In general, this extended experiment shows that the proposed Trust-based feature can enhance the learning capability of tree-based models under constrained configurations by providing one more indicator on the reliability of the data.

5.6 Comparison with Related Work

In this section, we compare our proposed model with previous studies.

5.6.1 Comparison with IoMT Review Literature

The reviewed study [81] provides a comprehensive and systematic overview of IoMT, its evolution, and role in enabling Smart Healthcare Systems through integrated devices, sensors, and software platforms. The paper discusses on a wide scale the integration of ML and AI techniques for the analysis of medical data, early disease diagnosis, predictive healthcare, and remote patient monitoring by presenting the employment of Random Forest, SVM, CNN, and ResNet models that represent the most useful applications-keeping in view COVID-19 diagnosis, medical image diagnosis, and elderly patient monitoring. In addition, the review emphases major challenges regarding data security, privacy, ethical concerns, and issues related to interoperability, scalability, and energy efficiency, together with a review of existing techniques and strategies for IoMT systems security and optimization of resources. However, the review paper does not propose or discuss the practical implementation or experimental frameworks of these theoretical insights. However, as a review paper, it does not present an implemented system or experimental evaluation. In contrast, our study focuses on a practical IoMT-based framework for secure ambulance-to-hospital patient data transmission, incorporating ML-based classification with Zero Trust security mechanism. Another study [83] on Cyberattack detection in IoMT using ML Techniques, proposes a comprehensive review on ML technology-based cyberattack detection in IoMT environments. This study focuses on existing algo-

rithms, datasets, issues, and gaps. The major differences with our work are that, while we proposed and implemented the effectiveness of a comprehensive integrated security framework using ML, ZTM, IDS, 2FA and medical data validation, this study did not propose any new algorithm or empirical testing on datasets. This study mainly focuses on binary form attack detection methods and gaps related to datasets, feasibility, and resource efficient models. Our study covers these lacunas by implementing multiclass classification, attack, normal, and medical issue, by leveraging IoMT relevant datasets, and proposing a real-time architecture suitable for edge environments. In addition, the reviewed work considers IoMT security from a primarily network-centric point of view, whereas our contribution extends the notion of security to data integrity, trust enforcement, and clinical decision support, hence making it more holistic and application oriented for IoMT cybersecurity.

5.6.2 Comparison with Studies Implementing ZTM in Healthcare

We compare our work with previous ZTM applications in healthcare systems to identify similarities, differences, and improvements. The two studies compared are [6] and [39], the key difference between our proposed model and these studis that our work focus on aplying ZTM on an mobile environment like ambulance by continuously monitoring both the data content and network traffic behavior to isolate any compromised IoMT device based on suspicious data behavior, while also isolating (as a concept) the ambulance's network interface in case of DDoS attack detected to contain threats at their source before they reach the hospital. Study [6] applied ZTM by a continuous authentication strategy, and the other study [39] focused on reducing medical errors by managing access in the cloud. Our study focuses on the

security of ambulance device data during transit and the detection of cyberattacks and distinguishing between attacks and medical issues. Accordingly, the two studies are complementary, as the former addresses the post-data arrival phase in the cloud, while our study addresses the real-time transmission phase. The table below 5.13 shows a summary comparison between these studies.

Table 5.13: Comparison between ZTCloudGuard and Our Study

Aspect	**Our Study**	**Study [39]**	**Study [6]**
Focus	Real-time protection of IoMT data in ambulances during transmission to hospitals. Depending on the behavior analysis of the network, with a focus on the data content level.	Aiming to reduce the medical errors by managing access in the cloud of the healthcare system using ZTM and a context-aware framework.	A lightweight continuous and mutual authentication framework for IoMT to ensure secure communication and device authentication
Healthcare Environment	Mobile (ambulance)	Static	Static
AI or ML used	ML	AI	No
Dataset used	Human Vital Sign Dataset with synthetic data, and ICU Healthcare Security Dataset	Synthetic dataset	-
Evaluation Metrics	Accuracy, Precision, F1-score, Recall, FPR, FNR, Time detection, memory usage, AUC, MCC and Cohen's Kappa.	F1-score, Precision, Recall	Computation cost, Communication overhead, Authentication delay, Energy consumption
ZTM Application Location	ZTM is applied at the edge (ambulance): Network segmentation, least privilege on use of IoMT devices and isolate the compromised device.	Cloud-based healthcare system for access management	Applied at the IoMT D2D and D2E communication level
Result	High accuracy nearly 98% with very short detection time, enabling real-time classification of normal, medical issues, and attacks at the data content level and the FPR decreased to nearly zero when compared with the trust score of the response action.	F1-score 93.5%, effective in preventing medical errors in cloud access management	The framework showed low computational cost, low communication overhead, and fast authentication time, making it suitable for IoMT environments.

5.6.3 Comparison with studies using the same dataset

At the network level:The study [55] used the same dataset (ICU Healthcare Security Dataset) as our work. However, while their study considered only two classes: attack and normal, our study analyzed three cases: DDoS attack, other attacks, and normal. In our experiments, the best overall accuracy was achieved by DT 99.65% and KNN 99.57%, with MCC values of 99.97 for DT and 99.2 for KNN. In contrast, the aim of the study in [55] was to distinguish between attack and normal only, achieving an accuracy of 99.51% with RF and AUC = 1.

At the Data Content level:The study [77], a recent work from 2025, used the Human Vital Sign Dataset from Kaggle to train and evaluate their ML models, reporting an accuracy of 99.0% for predicting patient health conditions, demonstrating strong generalization. In comparison, our study achieved 98.096% accuracy with DT, and integrating ZTM further enhanced security and robustness in IoMT systems.

5.6.4 Comparison with Other Datasets

Comparison Our Dataset with the WUSTL-EHMS-2020 Dataset

The WUSTL-EHMS-2020 dataset [58] was constructed by Washington University in St. Louis (WUSTL) researchers on a real-world testbed (EHMS), which is the nearest one to our dataset worked on. The dataset includes 16,318 records, with 14,272 of them being normal records and 2,046 of them being attack records. The dataset consists of two feature sets: network features and vital sign features. The attacks in the dataset include spoofing attacks, data injection attacks, and MitM attacks. This dataset is labeled only as normal or attack. Before applying to ML,

the dataset was preprocessed, cleaned, and the features were chosen.

In contrast our dataset at the data content level used is: Human Vital Sign Dataset from the Kaggle site [49] with vital signs features and synthetic attack simulation, ICU Healthcare Security Dataset from the Kaggle site [55], too, with network features and labeled to normal or attacks including DDoS attacks, while our dataset is labeled as normal, attack, or medical issue, and is separated from the network features for two main reasons. First, we did not find a comprehensive dataset that includes DDoS attacks, vital signs, and network features. Second, we aimed to apply ZTM to the network in order to temporarily isolate ambulances or IoMT devices when a data attack is detected, since it would be difficult to determine whether the detected abnormality originates from a network attack like DDoS or from a genuine medical issue related to the patient.

5.6.5 Comparison with Existing Hybrid Fog-Edge Approaches in IoMT Security

This study [45], which was explained in the literature under the section: Edge-Deployed Lightweight Security Models for IoMT. The referenced study aims to protect patient data and reduce latency by adopting a hybrid fog–edge–cloud architecture, where machine learning models are trained in the cloud, vital signs are collected and preprocessed at the edge, and the inference is executed in the fog. In contrast, our study deploys the trained model directly at the edge to enable real-time decision making. Also, our work emphasizes proactive alerting of medical staff whenever abnormal readings indicating a potential health issue are detected. Unlike the referenced study, we also utilized two separate datasets to cover both vital signs and

network-level attack scenarios, thereby providing a broader evaluation of IoMT security and reliability. The table below 5.14 shows a summary of the comparison between the two studies.

Table 5.14: Comparison between Hybrid Fog-Edge Study and Our Study

Aspect	**Hybrid Fog-Edge Study**	**Our Study**
The aim of the study	To solve 2 main issues: To minimize latency by applying Hybrid Fog-Edge computing, and secure patient data by an encryption mechanism.	To develop a real-time lightweight framework that includes ML, SIDS, ZTM, and 2FA to detect threats (DDoS and data injection) at both network and data levels, apply isolation mechanisms, and ensure security in EMS environments.
Dataset	IoT-health dataset from the Kaggle site with 250,000 records focusing on vital signs and anomaly detection.	Human Vital Sign Dataset with synthetic data for the data content level, and ICU Healthcare Security Dataset for the network level.
Classification Scheme	Binary classification: normal vs. anomaly.	Multi-class classification: normal, medical issue, attack at data level.
Threat Model	Focus on general security issues: unauthorized access, spoofing, data breaches.	Explicitly addresses DDoS and data injection attacks in IoMT systems.
Methodology	The proposed hybrid fog-edge architecture with 3 layers: Edge for collecting and processing vital signs, fog for the execution, and cloud for training ML models.	Integrating ML with ZTM to secure IoMT syesem, ML to train and classify the case while ZTM to apply the isolation for compromised device.
Results	Reduced latency by 70% compared to cloud and improved energy efficiency by 30%.	High accuracy nearly 98% with very short detection time, enabling real-time classification of normal, medical issues, and attacks at data content.

5.6.6 Comparison with Related Machine Learning-Based Works

There are several studies that applied machine learning approaches to intrusion detection at network or data content in healthcare services. The paper relying on an ELM-based approach in [82] deals with binary data DDoS intrusion detection in IoMT. The architecture has been optimized to limit computational cost and is appropriate for implementation at the fog level. However, in that context, aspects of trust enforcement, data validation in healthcare services, and multi-layer security measures were neglected. Another study presented in [80] work on multi-class intrusion detection in a regular network using traditional machine learning classifiers like SVM and NB during experiments employing the NSL-KDD data set as illusstrates on Table 5.15. The study was confined to providing just intrusion detection without dealing with data content in healthcare services. The focus of our work is to provide data content level security in healthcare IoMT services through integration of ML with an overall ZTM-based security architecture.

Table 5.15: Comparison with Related Machine Learning-Based Works

Aspect	**Our Study**	**Study [82]**	**Study [80]**
The aim of the study	Real-time attack detection in patient data transmission from ambulances to hospitals based on network behavior analysis and data content inspection.	This study proposes using an ELM classifier to detect DDoS attacks in IoMT systems, aiming for fast and accurate detection with low resource consumption and real-time deployment at the fog level.	This study aims to improve IDS accuracy and reduce misclassification rates in general network intrusion detection environments.
Dataset used	Human Vital Sign Dataset with synthetic data and ICU Healthcare Security Dataset.	CICIoMT 2024 dataset with 476,150 records.	NSL-KDD dataset.
ML models used	DT, RF, KNN, NB, and SVM classifiers.	Extreme Learning Machine classifier.	SVM classifier.
Binary or multiclass classification	Multiclass.	Binary (DDoS attack, Normal).	Multiclass.
Result	High accuracy of nearly 98% with very short detection time, enabling real-time classification of normal, medical issues, and attacks at the data content level, with near-zero FPR after trust-based response integration.	94.87% accuracy using the ELM classifier for IoMT traffic detection.	Best accuracy of 97.28% using the SVM classifier.

5.7 Summary

The proposed framework was partially implemented at the network level, implemented and completely evaluated in this chapter at the data content level. In the experiments, it was observed that the integration of ZTM, SIDS, ML, and 2FA supported real-time response and detection against injection attacks. At the data level,

ML models successfully classified among medical issues, normal situations, and cyberattacks. Metrics including: accuracy, precision, recall, detection time, and memory usage confirmed the efficiency of the DT, RF, and KNN models and rendered them most suitable for edge deployment in the case of classification, then integrated with ZTM to isolate the compromised device. In summary, the results confirm the feasibility of the suggested lightweight security framework in EMS environments.

Chapter 6

Conclusion and Future Work

6.1 Future Work and Limitations

Although our proposed model demonstrates that the work operates at both the data content and network levels, there are several future directions to improve it. In particular, the application was simulation-based, and we faced several limitations. To the best of our knowledge, there is no suitable dataset that simultaneously includes IoMT-derived vital signs and network features with specific attacks such as DDoS and injection attacks.

Furthermore, because the work was simulation-based, applying ZTM depended on the level compromised by attacks. Therefore, we generated synthetic attacks on vital signs to simulate a data content-level dataset. This limitation suggests a future direction: creating a dataset that includes all relevant features and additional types of attacks, such as MitM, to facilitate further improvements and integrate other IoMT devices, as we explained before the target is to build the framework and

further develop it because we use ML to be adaptable. Additionally, we aim to apply this framework in real-world scenarios. The focus in this work was primarily on data content, with less emphasis on network-level simulation, as described in Chapter 4. Therefore, future work could involve a deeper exploration of the network level to enhance the model further. We are planning to use AI to alert management to the response action.

6.2 Conclusion

In this thesis, we proposed a lightweight ML model for mobile environments, focusing on real-time processing at the edge in EMS, to simulate that we use: ZTM, 2FA, and SIDS. The target of this work is to continuously monitor both the network traffic behavior level and the data content behavior level. The primary focus was on the data content behavior level, where the system identifies whether an abnormality corresponds to an attack at a specific threshold or indicates a medical issue. Based on this, the system either triggers a security response or alerts the medical crew. Additionally, threats are isolated to prevent further impact before the data reaches the hospital, following the ZTM principle of 'Never trust, always verify.'In this context, the IoMT device from which the reading originates can be isolated from its network interface to contain the threat. At the network behavior level, the approach was considered as a descriptive idea, since it represents the first step before shifting to data content analysis. The focus was on detecting DDoS attacks, which indicate an external threat; once detected, the network interface of the ambulance was temporarily isolated after triggering the security response. Through simulation,

we demonstrated the effectiveness of the proposed system and aligned our work with recommendations from previous studies.

6.3 Recommendation

Based on our simulation results, we recommend that EMS, including their healthcare providers, integrate this lightweight model and deploy it on-board ambulances. It may be combined with security tools such as SIDS, 2FA, and ZTM alongside ML to potentially reduce possible threats affecting the security of EMS, especially patient data and to build adaptable framework to integrate another kinds of device or attack. We recommend implementing such a framework on multiple levels, as also suggested by other studies, and continuously training and updating the models to cover additional types of attacks. Finally, we believe that interventions for awareness and training for healthcare providers could increase the effectiveness of the system.

Bibliography

[1] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[3] G. Mouanda, "Comprehensive up-to-date impact of the IoMT in healthcare and patients," *arXiv preprint*, arXiv:2409.01287, 2024.

[4] C. R. Bhukya, P. Thakur, B. R. Mudhivarthi, and G. Singh, "Cybersecurity in Internet of Medical Vehicles: State-of-the-art analysis, research challenges and future perspectives," *Sensors*, vol. 23, no. 19, p. 8107, 2023.

[5] A. M. Almaazmi, S. H. Alhammadi, A. A. Al Ali, N. I. Alzaabi, and J. M. Kiklikian, "Riding to the rescue: A comprehensive review of health and safety measures in ambulance cars," *Int. J. Occup. Saf. Health*, vol. 14, no. 2, pp. 282–293, 2024.

[6] W. Almuseelem, "Continuous and mutual lightweight authentication for zero-trust architecture-based security framework in cloud-edge computing-based healthcare 4.0," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 1, 2024.

[7] B. Chowdhury, H. Jahankhani, and S. Subramaniam, "Zero-Trust Blockchain-Based Digital Twin 6G AI-Native Conceptual Framework Against Cyber Attacks for e-Healthcare," in *Proc. Int. Conf. Global Security, Safety, and Sustainability*, Springer, 2025, pp. 453–479.

[8] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. Kang Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers and Security*, vol. 103, p. 102150, 2021.

[9] K. S. Aryamol, F. J. Kurian, A. Shaji, A. Venkatesh, and M. M. James, "Smart ambulance with patient health monitoring," *Int. J. Adv. Comput. Sci. Technol.*, vol. 9, no. 7, pp. 61–65, 2020.

[10] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," *arXiv preprint*, arXiv:2501.07703, 2025.

[11] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4049, 2022.

[12] A. Rocha, M. Monteiro, C. Mattos, M. Dias, J. Soares, R. Magalhães, and J. Macedo, "Edge AI for Internet of Medical Things: A literature review," *Comput. Electr. Eng.*, vol. 116, p. 109202, 2024.

[13] M.-I. Joo, D.-Y. Kang, M.-S. Kang, and H.-C. Kim, "A Patient Management System Using an Edge Computing-Based IoT Pulse Oximeter," *Appl. Sci.*, vol. 14, no. 1, p. 414, 2024.

[14] Center for Internet Security, "DDoS attacks in the healthcare sector," *CIS Blog*, [Online]. Available: https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector. [Accessed: Jan. 17, 2025].

[15] O. AlShorman, B. AlShorman, M. Alkhassaweneh, and F. Alkahtani, "A review of Internet of Medical Things (IoMT)-based remote health monitoring through wearable sensors: A case study for diabetic patients," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 414–422, 2020.

[16] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the Internet-of-Medical-Things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, 2020.

[17] R. Hireche, H. Mansouri, and A. S. K. Pathan, "Security and privacy management in Internet of Medical Things (IoMT): A synthesis," *J. Cybersecur. Privacy*, vol. 2, no. 3, pp. 640–661, 2022.

[18] G. Choudhary and A. K. Jain, "Internet of Things: A survey on architecture, technologies, protocols and challenges," in *Proc. Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, 2016, pp. 1–8.

[19] A. Haghrah, M. P. Abdollahi, H. Azarhava, and J. M. Niya, "A survey on the handover management in 5G-NR cellular networks: aspects, approaches and challenges," *EURASIP J. Wirel. Commun. Netw.*, vol. 2023, no. 1, p. 52, 2023.

[20] S. Misra, C. Roy, and A. Mukherjee, *Introduction to Industrial Internet of Things and Industry 4.0*. Boca Raton, FL, USA: CRC Press, 2021.

[21] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," *Internet Things*, vol. 23, p. 100887, 2023.

[22] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," *Forrester Res. Inc.*, vol. 27, pp. 1–16, 2010.

[23] C. Buck, C. Olenberger, A. Schweizer, F. Völker, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Comput. Secur.*, vol. 110, p. 102436, 2021.

[24] Zero Security, "Zero Trust Security Principles," *ZeroSecurity.org*, [Online]. Available: https://zerosecurity.org/zero-trust-security-principles/14814/. [Accessed: Oct. 11, 2024].

[25] Microsoft, "What is two-factor authentication (2FA)?," *Microsoft Security*, [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa. [Accessed: May 20, 2025].

[26] M. O. Ahmad, G. Tripathi, F. Siddiqui, M. A. Alam, M. A. Ahad, M. M. Akhtar, and G. Casalino, "BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities," *Sensors*, vol. 23, no. 5, p. 2757, 2023.

[27] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013.

[28] M. Nankya, R. Chataut, and R. Akl, "Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies," *Sensors*, vol. 23, no. 21, p. 8840, 2023.

[29] S. Tariq, S. Lee, H. K. Kim, and S. S. Woo, "CAN-ADF: The controller area network attack detection framework," *Comput. Secur.*, vol. 94, p. 101857, 2020.

[30] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning based intrusion detection methods for Internet of Medical Things," *Appl. Soft Comput.*, vol. 140, p. 110227, 2023.

[31] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 160, 2021.

[32] Scikit-learn developers, "Tree-based models," *Scikit-learn Documentation*, https://scikit-learn.org/stable/modules/tree.html, accessed Jul. 10, 2025.

[33] IBM, "What is Random Forest?," *IBM Think Blog*, [Online]. Available: https://www.ibm.com/think/topics/random-forest. [Accessed: Jul. 10, 2025].

[34] IBM, "What is K-Nearest Neighbors (KNN)?," *IBM Think Blog*, [Online]. Available: https://www.ibm.com/think/topics/knn. [Accessed: Jul. 16, 2025].

[35] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, "An artificial intelligence approach for deploying zero trust architecture (ZTA)," *Proc. 5th Int. Conf. Comput. Inform. (ICCI)*, pp. 343–350, 2022.

[36] M. Al-Sharify, T. A. Al-Sharify, N. T. Al-Sharify, Z. T. Al-Sharify, A. T. Al-Sharify, M. A. Kareem, and A. M. K. Al-Dlaimi, "Employing the beamforming technique to enhance the medical ambulance performance, IoMT," *Tikrit J. Eng. Sci.*, vol. 32, no. 1, pp. 1–9, 2025.

[37] D. Rocha, G. Teixeira, E. Vieira, J. Almeida, and J. Ferreira, "A modular in-vehicle C-ITS architecture for sensor data collection, vehicular communications and cloud connectivity," *Sensors*, vol. 23, no. 3, p. 1724, 2023.

[38] V. Kavitha and P. Pon, "Smart ambulance for emergency cases to be reported to hospitals at the earliest using deep learning algorithms and blockchain-based distributed health record transactions for smart cities," in *Blockchain and IoT

Based Smart Healthcare Systems*, Bentham Science Publishers, 2024, pp. 244–259.

[39] K. Al-Hammuri, F. Gebali, and A. Kanan, "ZTCloudGuard: Zero trust context-aware access management framework to avoid medical errors in the era of generative AI and cloud-based health information ecosystems," *AI*, vol. 5, no. 3, pp. 1111–1131, 2024.

[40] G. Balhareth and M. Ilyas, "Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection," *Sensors*, vol. 24, no. 17, p. 5712, 2024.

[41] M. Asif, M. Abrar, A. Salam, F. Amin, F. Ullah, S. Shah, and H. AlSalman, "Intelligent two-phase dual authentication framework for Internet of Medical Things," *Scientific Reports*, vol. 15, no. 1, p. 1760, 2025.

[42] H. Rathore, C. Fu, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, and Z. Yu, "Multi-layer security scheme for implantable medical devices," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4347–4360, 2020.

[43] W. Almuseelem, "Secure latency-aware task offloading using federated learning and zero trust in edge computing for IoMT," *IEEE Access*, 2025.

[44] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT-based solutions for health care: Moving AI to the edge," *Pattern Recognit. Lett.*, vol. 135, pp. 346–353, 2020.

[45] U. Islam, M. N. Alatawi, A. Alqazzaz, S. Alamro, B. Shah, and F. Moreira, "A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience," *Sci. Rep.*, vol. 15, no. 1, p. 25655, 2025.

[46] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, "An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems," *IEEE Access*, vol. 8, pp. 107112–107123, 2020.

[47] E. Charbek, "Normal Vital Signs," *Medscape*, [Online]. Available: https://emedicine.medscape.com/article/2172054-overview. [Accessed: Jun. 8, 2025].

[48] Pindrop, "What is a personal identification number (PIN)?," *Pindrop Glossary*, [Online]. Available: https://www.pindrop.com/glossary/personal-identification-number/. [Accessed: Oct. 22, 2025].

[49] Kaggle, "Human Vital Sign Dataset," *Kaggle Datasets*, [Online]. Available: https://www.kaggle.com/datasets/nasirayub2/human-vital-sign-dataset. [Accessed: Oct. 25, 2025].

[50] Labris Networks, "The Critical Risk of DDoS Attacks in Healthcare: Proactive Mitigation with HARPP DDoS Mitigator," *Labris Networks Blog*, [Online]. Available: https://labrisnetworks.com/the-critical-risk-of-ddos-attacks-in-healthcare-proactive-mitigation-with-harpp-d [Accessed: Oct. 24, 2025].

[51] NETSCOUT, "Why Do Hackers Use DDoS Attacks?," *NETSCOUT Blog*, [Online]. Available: https://www.netscout.com/blog/why-do-hackers-use-ddos-attacks. [Accessed: Jun. 4, 2025].

[52] Y.-K. Lai, M.-H. Nguyen, and others, "A real-time DDoS attack detection and classification system using hierarchical temporal memory," *APSIPA Transactions on Signal and Information Processing*, vol. 12, no. 2, 2023, Now Publishers, Inc.

[53] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "MQTTset, a new dataset for machine learning techniques on MQTT," *Sensors*, vol. 20, no. 22, p. 6578, 2020, MDPI.

[54] MazeBolt, "ACK-PSH Flood," *MazeBolt Knowledge Base*, [Online]. Available: https://kb.mazebolt.com/knowledgebase/ack-psh-flood/. [Accessed: Oct. 1, 2025].

[55] Kaggle, "IoT Healthcare Security Dataset," *Kaggle Datasets*, [Online]. Available: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset. [Accessed: Oct. 26, 2025].

[56] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "A framework for malicious traffic detection in IoT healthcare environment," *Sensors*, vol. 21, no. 9, p. 3025, 2021, MDPI.

[57] N. Savanović, A. Toskovic, A. Petrovic, M. Zivkovic, R. Damaševičius, L. Jovanovic, N. Bacanin, and B. Nikolic, "Intrusion detection in healthcare 4.0 In-

ternet of Things systems via metaheuristics optimized machine learning," *Sustainability*, vol. 15, no. 16, p. 12563, 2023, MDPI.

[58] R. Jain, "WUSTL-EHMS-2020 Dataset: Enhanced Healthcare Monitoring System (EHMS)," *Washington University in St. Louis*, [Online]. Available: https://www.cse.wustl.edu/~jain/ehms/index.html. [Accessed: Aug. 30, 2025].

[59] M. Jaradat and I. Ishaq, "Smart Health Monitoring System for Elderly Palestinians Using Internet of Things (IoT)," *Preprints*, 2024.

[60] S. Elkilany, "A Wearable-Based Hidden Markov Model for Health Monitoring in Conflict Zones: A Case Study of Gaza," 2025.

[61] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-in-the-middle attack mitigation in internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2053–2062, 2021, IEEE.

[62] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, and R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," *Applied Soft Computing*, vol. 118, p. 108439, 2022, Elsevier.

[63] Pritika, B. Shanmugam, and S. Azam, "Risk evaluation and attack detection in heterogeneous IoMT devices using hybrid fuzzy logic analytical approach," *Sensors*, vol. 24, no. 10, p. 3223, 2024, MDPI.

[64] Z. ElSayed, A. Abdelgawad, and N. Elsayed, "CryptoDNA: A Machine Learning Paradigm for DDoS Detection in Healthcare IoT, Inspired by crypto jacking prevention Models," *arXiv preprint arXiv:2501.18549*, 2025.

[65] J. Opitz and S. Burst, "Macro F1 and macro F1," *arXiv preprint arXiv:1911.03347*, 2019.

[66] Evidently AI, "Classification Metrics Guide," [Online]. Available: https://www.evidentlyai.com/classification-metrics. [Accessed: Oct. 29, 2025].

[67] S. Sathyanarayanan and B. R. Tantri, "Confusion matrix-based performance evaluation metrics," *African Journal of Biomedical Research*, vol. 27, no. 4S, pp. 4023–4031, 2024.

[68] O. Rainio, J. Teuho, and R. Klén, "Evaluation metrics and statistical tests for machine learning," *Scientific Reports*, vol. 14, no. 1, p. 6086, 2024, Nature Publishing Group UK.

[69] H. Goonewardana, "Evaluating multi-class classifiers," *Apprentice Journal (Medium)*, Jan. 3, 2019. [Online]. Available: https://medium.com/apprentice-journal/evaluating-multi-class-classifiers-12b2946e755b. [Accessed: Nov. 27, 2025].

[70] V. Trevisan, "Multiclass classification evaluation with ROC Curves and ROC AUC," *TDS Archive (Medium)*, 2022. [Online]. Available: https://medium.com/data-science/

multiclass-classification-evaluation-with-roc-curves-and-roc-auc-294fd4617e3a. [Accessed: Nov. 27, 2025].

[71] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: Threats, mitigation and approaches," *BMJ Health & Care Informatics*, vol. 26, no. 1, p. e100031, 2019.

[72] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, "CT-GAN: Malicious tampering of 3D medical imagery using deep learning," in *Proc. 28th USENIX Security Symp. (USENIX Security 19)*, pp. 461–478, 2019.

[73] F. Abtahi, F. Seoane, I. Pau, and M. Vega-Barbas, "Data poisoning vulnerabilities across healthcare AI architectures: A security threat analysis," *arXiv preprint arXiv:2511.11020*, 2025.

[74] G. A. Gellert, D. Borgasano, R. Palermo, G. L. Gellert, and S. P. Kelly, "Third-party access cybersecurity threats and precautions: A survey of healthcare delivery organizations," *Applied Clinical Informatics*, vol. 16, no. 5, pp. 1518–1530, 2025.

[75] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," *Symmetry*, vol. 15, no. 11, p. 1981, 2023.

[76] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. A. Khan, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, 2020.

[77] U. H. Khan, A. Qamar, R. Khan, F. Alturise, A. R. Alshaabani, and S. Alkhalaf, "Secure edge-based IoMT framework for ICU monitoring with TinyML and post-quantum cryptography," *Sci. Rep.*, vol. 15, no. 1, p. 36195, 2025.

[78] S. Saif, P. Das, S. Biswas, S. Khan, M. A. Haq, and V. Kovtun, "A secure data transmission framework for IoT enabled healthcare," *Heliyon*, vol. 10, no. 16, 2024.

[79] J. R. Suchard, "Recovery from severe hyperthermia (45 C) and rhabdomyolysis induced by methamphetamine body-stuffing," *West. J. Emerg. Med.*, vol. 8, no. 3, p. 93, 2007.

[80] A. Halimaa and K. Sundarakantham, "Machine learning based intrusion detection system," in *Proc. 3rd Int. Conf. on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2019, pp. 916–920.

[81] G. R. Pradyumna, R. B. Hegde, K. Bommegowda, T. Jan, and G. R. Naik, "Empowering healthcare with IoMT: Evolution, machine learning integration, security, and interoperability challenges," *IEEE Access*, vol. 12, pp. 20603–20623, 2024.

[82] N. Elsayed, L. Dzamesi, Z. ElSayed, and M. Ozer, "Extreme learning machine based system for DDoS attacks detections on IoMT devices," *arXiv preprint arXiv:2507.05132*, 2025.

[83] M. Narang, A. Jatain, and N. Punetha, “A study on cyber-attack detection in IoMT using machine learning techniques,” in *Proc. Int. Conf. on Innovative Computing & Communication (ICICC)*, 2022.

Appendix A

Training Dataset (Data Content Level)

Table A.1: Training Dataset Used at Data Content Level

Patient ID	Heart Rate	Respiratory Rate	Body Temperature	Oxygen Saturation	Systolic BP	Diastolic BP	Derived BMI	Risk Category	Abnormal Type	Trust Score
2900070	188	43	37.702	98	151	80	24.644	Abnormal	Medical Issue	0.2
2900071	178	39	36.0	97	140	80	29.696	Abnormal	Medical Issue	0.2
2900072	164	43	36.03	95	158	81	24.001	Abnormal	Medical Issue	0.2
152147	73	15	36.8	95.52	110	80	25.768	Normal	Normal	0
2900074	157	31	36.72	99	156	80	23.818	Abnormal	Medical Issue	0.1
2900075	170	41	36.77	99	144	82	28.152	Abnormal	Medical Issue	0.2
2900076	188	35	37.12	99	142	79	25.877	Abnormal	Medical Issue	0.1
2900077	168	40	36.38	98	141	80	25.882	Abnormal	Medical Issue	0.2
2900078	172	30	36.42	99	142	81	29.390	Abnormal	Medical Issue	0.1
2900079	160	32	36.96	95	147	81	29.145	Abnormal	Medical Issue	0.1
2900080	160	34	37.50	99	155	82	24.940	Abnormal	Medical Issue	0.1
2900081	173	33	37.23	96	145	79	24.234	Abnormal	Medical Issue	0.1
2900082	185	32	36.59	99	152	82	28.654	Abnormal	Medical Issue	0.1
2900083	189	39	36.86	98	155	79	29.0518	Abnormal	Medical Issue	0.2
2900084	173	42	36.34	96	155	81	26.533	Abnormal	Medical Issue	0.2
2900085	152	34	36.14	95	142	82	27.140	Abnormal	Medical Issue	0.1
2900086	171	40	37.56	95	152	81	24.565	Abnormal	Medical Issue	0.2
2900087	151	37	36.53	97	153	81	28.324	Abnormal	Medical Issue	0.2
2900088	173	40	36.35	96	147	79	27.158	Abnormal	Medical Issue	0.2
2900089	193	45	37.38	97	151	82	26.270	Abnormal	Medical Issue	0.2
2900090	179	33	37.23	96	160	82	23.205	Abnormal	Medical Issue	0.1
2900091	187	30	37.266	96	147	81	29.120	Abnormal	Medical Issue	0.1
2900092	151	40	36.45	98	160	81	27.0436	Abnormal	Medical Issue	0.2
2900093	170	36	36.46	97	148	79	24.1218	Abnormal	Medical Issue	0.2
2900094	182	37	36.44	98	140	82	26.9810	Abnormal	Medical Issue	0.2
2900095	161	32	36.34	96	145	80	27.472	Abnormal	Medical Issue	0.1
2900096	171	35	37.31	95	158	81	26.423	Abnormal	Medical Issue	0.1
2900097	193	31	37.69	96	150	80	27.753	Abnormal	Medical Issue	0.1
220314	82	15	44.49	95.47	121	90	21.27	Abnormal	Attack	0.1
220315	66	44	37.27	96.41	130	81	22.38	Abnormal	Attack	0.1
220316	72	57	37.35	95.01	122	74	21.84	Abnormal	Attack	0.1
220317	68	44	36.7	97.95	125	89	20.82	Abnormal	Attack	0.1
220318	172	18	37.1	95.96	128	72	25.43	Abnormal	Attack	0.1
220319	172	17	37.08	98.92	126	90	22.81	Abnormal	Attack	0.1
220320	74	18	44.09	95.92	123	85	25.04	Abnormal	Attack	0.1
220321	100	14	44.1	98.35	138	74	27.15	Abnormal	Attack	0.1
220322	92	59	37.42	95.19	110	85	19.38	Abnormal	Attack	0.1
220323	166	18	37.12	98.62	111	90	22.21	Abnormal	Attack	0.1
220324	64	47	37.32	95.42	139	73	23.28	Abnormal	Attack	0.1
220325	91	12	43.16	96.86	117	87	21.89	Abnormal	Attack	0.1
220326	94	55	36.74	95.05	119	87	24.96	Abnormal	Attack	0.1
220327	182	20	36.84	96.71	135	88	27.67	Abnormal	Attack	0.1
220328	153	14	36.99	95.9	128	84	23.84	Abnormal	Attack	0.1
220329	98	36	36.54	97.7	125	88	25.57	Abnormal	Attack	0.1
220330	71	14	44.58	98.54	136	89	26.89	Abnormal	Attack	0.1
220331	182	15	36.6	97.13	134	71	23.94	Abnormal	Attack	0.1
220332	73	36	36.81	95.77	133	88	27.43	Abnormal	Attack	0.1
220333	180	16	36.58	95.51	112	87	27.63	Abnormal	Attack	0.1
220334	184	19	36.8	96.46	134	77	27.86	Abnormal	Attack	0.1
220335	150.0	37.04	43.84	98.83	110	77	19.29	Abnormal	Attack	0.3
200573	150.31	38.9	44.71	98.62	132	83	21.64	Abnormal	Attack	0.3
220337	86	56	37.42	98.55	116	79	28.63	Abnormal	Attack	0.1
220338	66	56	36.83	97.96	117	87	22.63	Abnormal	Attack	0.1
220339	68	12	43.65	95.82	139	78	25.96	Abnormal	Attack	0.1
220340	73	16	43.57	95.5	120	76	21.18	Abnormal	Attack	0.1
220341	176	15	37.13	96.13	117	72	25.31	Abnormal	Attack	0.1
220342	100	20	43.2	97.85	130	84	24.51	Abnormal	Attack	0.1