Enhancing IoMT Security Using Multi-Layer Authentication: A Zero-Trust Machine Learning Case Study for Emergency Medical Services

1st Basma Mohammad Abu Sabha
Department of Informatics
Palestine Polytechnic University
Hebron, Palestine
Email: 216062@ppu.edu.ps

2nd Radwan Tahboub
Vice President for IT and Digital Transformation
Palestine Polytechnic University
Hebron, Palestine
Email: radwant@ppu.edu

***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 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, they do not focus on detecting anomalies during transmission or analyzing network and data content behavior in real-time. This paper proposes a real-time security framework for Emergency Medical Services (EMS) that 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 in detail at this level.**

Once an attack is detected, the system applies an isolation mechanism that either isolates the compromised IoMT device from it's 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. 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%. 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%.

***Index Terms*—Internet of Medical Things (IoMT), Zero Trust Model (ZTM), Two-Factor Authentication (2FA), Emergency Medical Services (EMS), Machine Learning (ML), Distributed Denial of Service (DDoS), Signature Intrusion Detection System (SIDS).**

I. Introduction

The 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].

Internet of Medical Things (IoMT) is a growing part of IoT, where devices, sensors, and software are combined to enable the acquisition and sharing of medical data. IoMT can revolutionize healthcare by introducing advanced diagnostic 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 [3]. In healthcare systems, medical environments can be classified as either static, such as hospitals, or mobile, such as the 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 Emergency Medical Services (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 study, 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 patient 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, making them attractive targets for cyberattacks such as malware and Distributed Denial of Service (DDoS) [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 behavior), 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 computational 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 e.g., 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 study 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 Machine Learning (ML), a Signature Intrusion Detection System (SIDS), the Zero Trust Model (ZTM), and Two-Factor Authentication (2FA). It achieves this by analyzing both data 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.

II. 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 [14], [15].

A. 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 1.

Fig. 1. The layers in IoMT architecture [16].

- Perception Layer: The foundational layer reads and collects health-related data using sensors and IoMT devices such as pacemakers, smartwatches, and oximeters. These devices transmit raw data to the network layer without processing [14].

- 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 IoT (NB-IoT), Bluetooth, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), ZigBee, and 5G NR (New Radio), 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 [17], [18].

- 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 [19].

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, such as smartphones and gateways, which in our work are inside the ambulance.
3. Cloud: It has powerful processing and unlimited storage, allowing it to handle the registration of all medical devices, and it also manages both the devices and edge nodes by securely storing their real identities level [3], [12].

B. 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, such as sniffing attacks and access control attacks. Ransomware and malware attacks will primarily affect the storage and cloud layers, in that data goes missing or becomes corrupted. Other attacks, like injection and password-based attacks, try to break through login systems and user access controls [10], [20]. In this study, we focus on detecting DDoS attacks and analyzing the content of the data to catch any signs of injection or tampering, especially in the case of smart ambulances.

C. Integration of Advanced Technologies in EMS System

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 [21] 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 [22]. 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 [23]:
1. 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.
2. Least Privilege Access: Grants users only the minimum access needed for their tasks, limiting potential damage if an account is compromised.
3. Micro-Segmentation: Micro-segmentation divides the network into isolated zones, limiting an attacker's lateral movement and minimizing potential impact.
4. Continuous Monitoring and Validation: Detecting unusual activities after behavioral analysis and logging instead of assuming granted access is always safe.

2. 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 [24]. Authentication factors can generally be classified into three traditional categories as follows [25]:

- 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.

3. Machine Learning with Feature Selection:
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 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 preprocessing to improve attack detection. Three categories of ML can be utilized in solving IoMT security issues.

- 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 [26].

In this study, we used lightweight ML such as RF, DT, NB, and KNN because of the test at the edge node, not at the cloud. Feature selection is applied to an easily available dataset to reduce input variables, improve efficiency, and decrease computational loads. Processes and simplifies the data, reduces dimensions, and focuses on crucial features [27].

4. 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 [28].

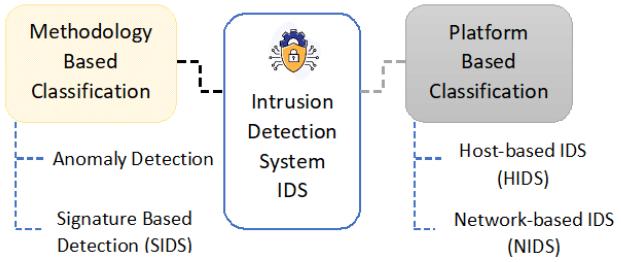

Fig. 2. Intrusion Detection Methodologies

In general, IDS can be categorized in two ways, as illustrated in Figure 2:
1) Classification by methodology.
2) 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 [29]. In our proposed model, we used SIDS when training the model on the cloud to determine the specific intrusion at the data content level.

Study [30] 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.

III. Literature Overview

The primary objective of AI is to enhance cybersecurity. Organizations are increasingly turning to AI to withstand emerging cybersecurity threats, technological problems, and lack of resources, increasing system strength, resilience, and response [31]. AI protects IoT/IoMT by adopting machine learning, deep learning, and natural language processing. It detects unusual behavior, makes decisions in real time, and can automatically react to threats, thereby improving the capability of the network to operate under dynamic conditions [32]. The healthcare environment includes various IoMT devices, among which ambulances represent one of the most critical components. Despite their importance, limited research specifically addresses the security of IoMV or ambulance systems [4]. Therefore, the research papers are divided into two groups: cybersecurity for mobile medical environments and cybersecurity for static medical environments.

- Cybersecurity for mobile medical environments: In a recent paper [33], the researchers aimed to improve the operation of medical ambulances in real-time and healthy safety areas by using 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 study [34] 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 IoV environment, ignoring 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. Another study [35] proposed a smart ambulance system for emergency cases in smart cities, integrating deep learning algorithms and blockchain-based distributed health record transactions. Deep learning algorithms were used to predict patient injuries, and blockchain technology ensured the integrity, privacy, and security of health data during transfer. Their study does not address attack detection or network behavior analysis. 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 helps physicians make 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.

- Securing patient data in a hospital environment:

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. Compared to this work, they work on ZTM based on authentication; 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. The researchers [36] proposed a context-aware ZTM access framework to reduce medical errors in cloud-based healthcare systems using machine learning for runtime data analysis; it assesses access requests to improve secure access control, addressing challenges in the vulnerable healthcare landscape. Another study [37] presented the Soter authentication system, which was based on IoMT zero trust. Soter integrates trust negotiation mechanisms within the ZTM for the dynamic establishment of trust. A negotiation process is initiated whenever a user or device requests access to a certain resource in which credentials, attributes, and contextual information are exchanged between the requester and the resource owner. An optimized IDS for IoMT networks was proposed [38] using tree-based machine learning classifiers and filter-based feature selection techniques. The paper was based on the Canadian Institute for Cybersecurity Intrusion Detection Dataset 2017 (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. It was not a real-time medical context. Moreover, SIDS finds a new application as a threshold-setting mechanism to distinguish cyberattacks from genuine medical emergencies based on abnormal vital signs to enhance detection reliability in life-critical scenarios.

IV. Problem Definition

In ambulances, which are mobile EMS environments with IoMT devices, the vital signs of patients are sent to hospitals in real time for immediate decision-making. These transmissions are, nevertheless, vulnerable to cyberattacks that can compromise patient safety even before reaching the hospital. A report from CyberPeace describes how attacks on the healthcare system, in which DoS/DDoS attacks are included, affect the delivery of basic care, delay operations, and endanger patient safety [39]. While most studies focus on hospital data security, few address securing communication between ambulances and hospitals in emergency systems [4]. In many of these studies, blockchain [40], [35] or various encryption protocols [41] are employed to secure data. These approaches, however, often assume the data is trustworthy without analyzing its behavior or source in real time. Moreover, current safety and cybersecurity standards, such as ISO 26262 and ISO 14971, do not sufficiently mitigate the risks of deploying IoMT devices in mobile environments like ambulances, nor do they offer clear frameworks for the secure and real-time transmission of vital signs. Additionally, medical personnel often lack well-defined risk management strategies for handling network-enabled devices [4]. This study addresses that critical gap by proposing a real-time intrusion detection approach that targets two levels of attack:
1. At the network level, it detects the DDoS attacks that attempt to block or flood the edge node communication channel before it gets transmitted to the hospital.
2. At the data level, it identifies injection attacks, where malicious or falsified medical data is sent from compromised devices.

The proposed model in this paper monitors network behavior as well as data content, identifies an attack after determining the attacked device (in the case of injection) or the network interface for the ambulance (in the case of DDoS), and actively isolates using ZTM.

V. Proposed Model

1. System Architecture

The system architecture of the proposed model is illustrated in Figure 3, consisting of:

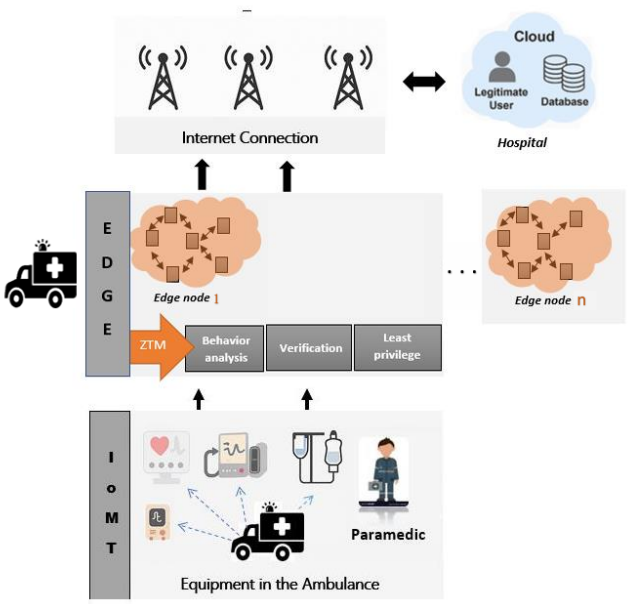

Fig. 3. Overview of Proposed System Architectur

- IoMT Devices : Such as oximeters, heart rate monitors, and respiratory rate sensors.
- Edge node: Closer to where the data is generated instead of relying only on distant cloud servers helps IoMT devices by providing extra processing and storage power, such as smartphones and gateways, which in our work are inside the ambulance.
- Cloud: In this model, the cloud layer represents the hospital.

2. **Flowchart of the Proposed System Model**

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 as illustrated in Figure 4.

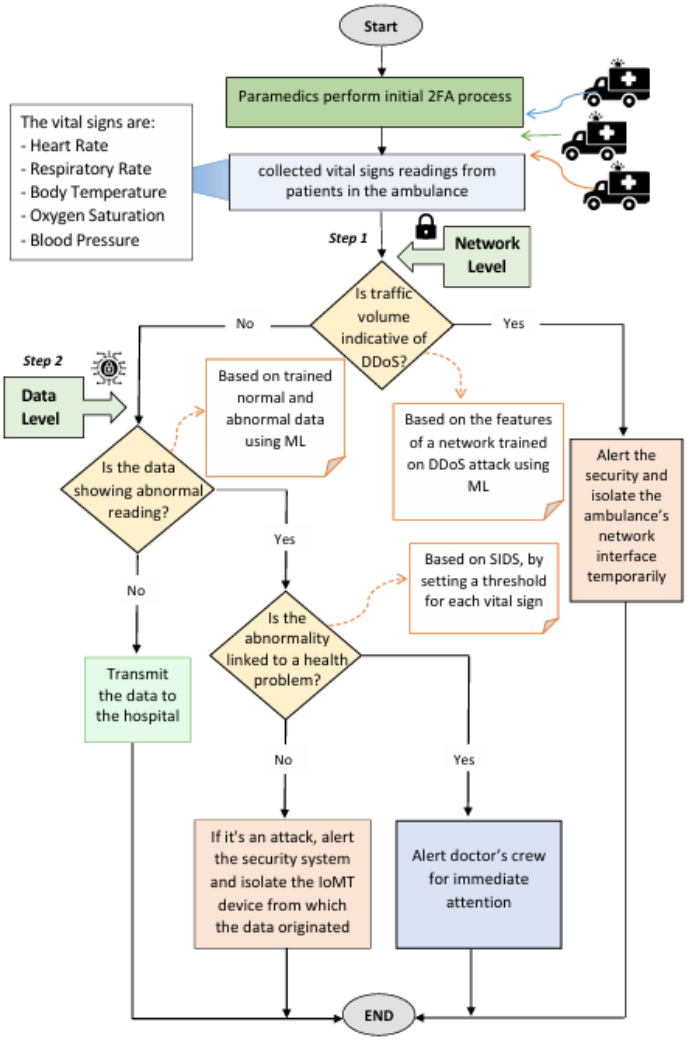

Fig. 4. Proposed System Model

The vital signs of the patient will be collected in the ambulance by paramedics after performing 2FA to access the devices. The proposed model works in two steps. 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 trigger security alerts.
These steps can be summarized in Algorithm 1 and 2.

Algorithm 1 Network-Level After 2FA

Precondition: Paramedic successfully logged in through 2FA
Input: Network traffic features
Output: Network status (Normal / DDoS Attack / Other Attack)
Apply ML model to classify network traffic
if Classification = DDoS Attack **then**
    Alert security team
    Isolate external network interface
else if Classification = Other Attack **then**
    Alert security team
else
    Proceed to Data-Level analysis
end if

This algorithm describes the network level security process performed after successful 2FA authentication, where ML is used to detect DDoS and other network attacks in the specific dataset used before allowing data content level processing.

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

The parameters $conf_high$ and $conf_medium$ represent predefined trust thresholds determined during experimental validation. Values above $conf_high$ trigger immediate iso-

lation, while values between $conf_medium$ and $conf_high$ indicate moderate risk.

The second step illustrates the check security model at the edge, incorporating the ZTM and 2FA as shown in Figure 5.

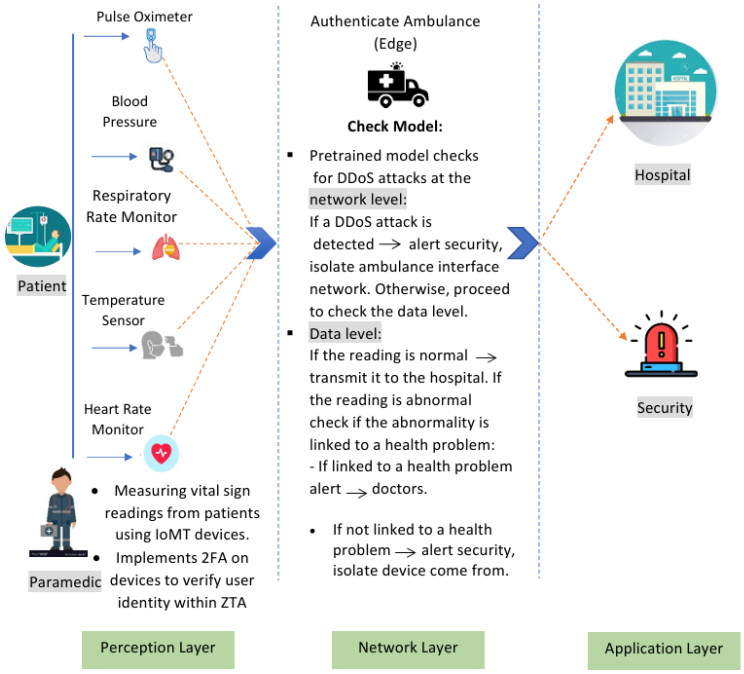

Fig. 5. Pretrained Security Model Deployed at the Edge for Ambulance System

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.

VI. Research Methodology

Our study introduces an IoMT security framework using ML, ZTM, SIDS, and 2FA to protect patient vital signs during EMS. Due to limited infrastructure, the framework was simulated in Python. At the data level, the simulation assessed the system's ability to isolate compromised IoMT devices based on data content behavior, confirming the effectiveness of ZTM, SIDS, and ML models in detection.

1. Dataset Description: At network level we used ICU Healthcare Security Dataset [42], 188,695 rows, with network features. Data preprocessing included handling missing values, normalization, and removal of irrelevant attributes to improve classification performance. This dataset 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. Other attacks which are the remaining attacks at this dataset used without analyzing them in depth. The DDoS class is defined based on known characteristics such as high message rates, redundancy, and abnormal traffic patterns, distinguishing it from other attacks. This dataset was chosen because it includes network features used in transmitting vital signs, which makes it suitable for the context of this work.

Data content level: Human Vital Sign Dataset [43], 200,000 rows, 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 clinical relevance: heart rate (HR), respiratory rate (RR), body temperature, oxygen saturation (SpO_2), systolic blood pressure, diastolic blood pressure (DBP), and derived BMI, which is the difference between height and weight. According to medically accepted threshold values, as reflected in the dataset, vital signs were classified as normal or abnormal based on standard clinical ranges.

- 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.

After that, it was modified with 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 according to study [44] , resulting in a new total dataset of 283,120 records. 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 condition. Therefore, 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. Lightweight classifiers such as DT, RF, and KNN were selected due to their suitability for real-time IoMT ambulance environments.

2. Attack Threat

Network level attacks: The attackers are external DDoS networks, 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.
Data content level attacks: 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 with absence of physiological consistency across all readings, this indicates that the data have been tampered with.

Assumptions: The paramedic is permitted to use the system but is not considered trusted by default, and therefore must complete a 2FA process before accessing the medical devices. Additionally, it is assumed that technical issues may occur in the medical devices during operation.

3. Data Content-Level Attacks Simulation: A simple simulation attack generation method was used to train the ML model to detect data-level spoofing attacks or injections. If a reading exceeds normal values, it may indicate an injection attack or a technical issue. In rare cases, it could correspond to a real medical condition. ML models are used to distinguish between these scenarios by checking for inconsistencies across all physiological readings.

4. System Design: The framework simulates a secure IoMT environment that integrates the following components:
- ZTM: Implement to isolate based on data content behavior and network traffic and then logging. First, if there is an attack on the network, the ambulance's network interface or connection point is isolated; otherwise, check the data content. If the attack occurred based on the content, the IoMT device from which the reading came will be isolated. This is why we work on two separate levels.
- SIDS: We will apply SIDS at the data level to analyze vital signs, detect anomalies, and determine whether they indicate a cyberattack or a healthcare issue.
- 2FA: To enhance access security, the paramedic will use email-based and SMS-based One-Time Passwords (OTPs) as part of the two-factor authentication process at access points.
- ML integrated: Machine learning is used to distinguish between a medical issue and a cyberattack based on the values of vital signs received from each medical device and to evaluate the overall framework. Training data may be performed in the cloud, while processing occurs at the edge node.

5. Testing: The dataset was divided into 70% training data and 30% testing data. The trained model was then tested on unseen IoMT data to replicate real-world situations and evaluate its ability to detect abnormal behavior such as DDoS attacks or data anomalies. In addition, 5-fold cross-validation was applied to ensure robust and reliable ML model evaluation, with results consistent with the test-set performance.

6. Evaluation Metrics: After testing, system performance is quantitatively assessed using evaluation metrics such as macro average for: Accuracy, Precision, Recall, F1-score. FPR (False Positive Rate), FNR (False Negative Rate) for each class, and MCC.

VII. Initial Findings

The results are reported separately for each level, in this paper we focus on data content level using a three-class classification setting (Normal, Medical Issue, and Attack). Table I shows the performance of the top three ML models.

TABLE I
Performance Summary of the best three ML Models for Multi Classification

Model	Acc	Prec	F1	Rec	MCC
DT	98.096	98.386	98.04	97.804	97.172
RF	98.01	98.093	98.119	98.238	97.055
KNN	97.724	97.849	97.861	97.875	96.56

High accuracy values confirm the effectiveness of the proposed three-class classification at the data content level, as indicated by the strong performance of the DT 98.096% then RF 98.01%, and KNN 97.724% classifiers.The Naïve Bayes model achieved 91.703%, while the Linear SVM performed relatively lower with 75.25% accuracy. The Matthews Correlation Coefficient (MCC) values show a high level of agreement between the actual and predicted classes for all models, indicating a reliable classification performance.

Detection time and accuracy were also evaluated, which helped assess the efficiency of the model. Figure 6 shows the relationship between the detection time and the accuracy.

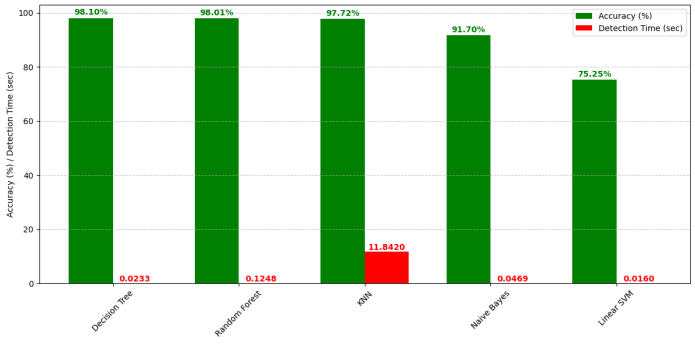

Fig. 6. Illustrates Models Accuracy and Detection Time

Though accuracy ensures proper classification, the detection time also plays an important role, as the lower the time, the better the response. Detection time, as shown in Equation 1, is critical in EMS settings where fast, reliable responses are required.

$$\text{Detection Time} = t_{\text{decision}} - t_{\text{start}} \tag{1}$$

- t_{start}: The time at which data analysis begins.
- t_{decision}: The time at which the anomaly is detected or classified.

The KNN model had the longest detection time, taking 11.842 seconds. DT demonstrated the best balance between high accuracy and low detection time, making it the most suitable model for real-time detection scenarios.

The FPR and FNR were computed for each class to analyze false positives and false negatives in the multi-class setting as illustrates in Table II.

TABLE II
FPR AND FNR PER EACH CLASS FOR TOP THREE ML MODELS

Class	DT FP	DT FN	RF FP	RF FN	KNN FP	KNN FN
Normal	0.00004	0.00002	0.0276	0.00011	0.01895	0.03021
Medical Issue	0.03020	0.00056	0.0008	0.0527	0.01618	0.03352
Attack	0.00026	0.06532	0.00210	0.0004	0.0001	0.00004

DT, RF, and KNN maintain low FPR and FNR for Normal, Medical Issue, and Attack classes, demonstrating consistent and accurate predictions.

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 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.

After integrating ZTM into the ML results, as outlined in Algorithm 2, the performance of KNN slightly improved, with accuracy increasing from 97.72% to 97.73%.For RF since the FPR was already very small, the effect of ZTM on this model was not clearly observable, also for DT, the overall accuracy remained unchanged, as it had already achieved a very low false positive rate, as shown in Table II. To further evaluate the impact of ZTM, we applied it to DT models trained at different depths as illustrates in Figure 7. The results indicate that integrating ZTM significantly improved DT performance: at depth 2, accuracy increased from 61.02% to 89.84%, and at depth 4, it rose from 89.08% to 95.34%.These results confirm the effectiveness of the ZTM approach in enhancing model performance.

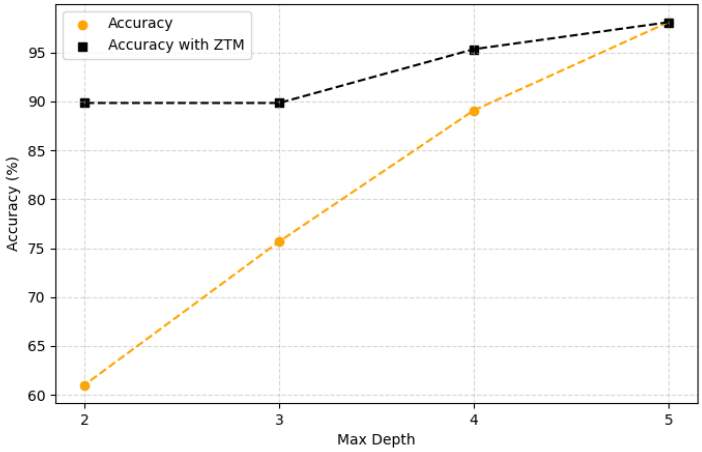

Fig. 7. Illustrates model accuracy in classifying system responses

VIII. Discussion

From the above results, it is clear that the use of ML, ZTM, SIDS, and 2FA technologies can enhance the security of IoMT based EMS environments. The proposed DT model offered a perfect combination between computational speed and classification accuracy, making it suitable for real-time ambulance systems. In addition, the framework provides dual-level protection by analyzing both network traffic and medical data behavior. However, the study used partly simulation for the attack scenario in the IoMT environment. Although more advanced methods like XGBoost and deep learning provided a higher level of accuracy, ML models were chosen due to cost effectiveness.

IX. Summary

In this thesis, we proposed a security framework for IoMT systems in EMS, 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 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, and future work will focus on the level of network traffic. A pre-trained, edge-deployed artificial intelligence model supports real-time anomaly detection and then integrated with ZTM to apply isolation decisions. The initial results show that the DT, RF, and KNN classifiers were evaluated at the edge for real-time multiclass classification, with DT achieving the highest accuracy 98.10% and MCC 97.17%. Through simulation, we demonstrated the effectiveness of the proposed system and aligned our work with recommendations from previous studies.

References

[1] Kevin Ashton et al. That 'internet of things' thing. *RFID journal*, 22(7):97–114, 2009.

[2] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: application areas, security threats, and solution architectures. *IEEe Access*, 7:82721–82743, 2019.

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

[4] Chidambar Rao Bhukya, Prabhat Thakur, Bhavesh Raju Mudhivarthi, and Ghanshyam Singh. Cybersecurity in internet of medical vehicles: State-of-the-art analysis, research challenges and future perspectives. *Sensors*, 23(19):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. *International Journal of Occupational Safety and Health*, 14(2):282–293, 2024.

[6] W. A. L. E. E. D. Almuseelem. Continuous and mutual lightweight authentication for zero-trust architecture-based security framework in cloud-edge computing-based healthcare 4.0. *Journal of Theoretical and Applied Information Technology*, 102(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 *International Conference on Global Security, Safety, and Sustainability*, pages 453–479. Springer, Cham, 2025.

[8] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & security*, 103:102150, 2021.

[9] K. S. Aryamol and F. Joe. Smart ambulance with patient health monitoring. *International Journal of Advanced Computer Science and Technology*, 9(7):1–5, 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). *Transactions on Emerging Telecommunications Technologies*, 33(6):e4049, 2022.

[12] Atslands Rocha, Matheus Monteiro, César Mattos, Madson Dias, Jorge Soares, Regis Magalhães, and José Macedo. Edge ai for internet of medical things: A literature review. *Computers and Electrical Engineering*, 116:109202, 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. *Applied Sciences*, 14(1):414, 2024.

[14] 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. *Indonesian Journal of Electrical Engineering and Computer Science*, 20(1):414–422, 2020.

[15] 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 of Things Journal*, 8(11):8707–8718, 2020.

[16] R. Hireche, H. Mansouri, and A. S. K. Pathan. Security and privacy management in internet of medical things (iomt): A synthesis. *Journal of Cybersecurity and Privacy*, 2(3):640–661, 2022.

[17] G. Choudhary and A. K. Jain. Internet of things: A survey on architecture, technologies, protocols and challenges. In *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pages 1–8. IEEE, December 2016.

[18] 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 Journal on Wireless Communications and Networking*, 2023(1):1–57, June 2023.

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

[20] 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 of Things*, 23:100887, 2023.

[21] J. Kindervag. Build security into your network's dna: The zero trust network architecture. Technical Report 27, Forrester Research Inc, 2010.

[22] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110:102436, 2021.

[23] Christi. Zero trust security: Principles of the zero trust security model, October 2024. Accessed: 2025-02-06.

[24] Microsoft. What is two-factor authentication (2fa)? https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa, n.d. Accessed: 2025-05-20.

[25] 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*, 23(5):2757, 2023.

[26] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia. Survey of machine learning based intrusion detection methods for internet of medical things. *Applied Soft Computing*, 140:110227, 2023.

[27] A. Islam, S. Seth, T. Bhadra, S. Mallik, A. Roy, A. Li, and M. Sarkar. Feature selection, clustering, and iomt on biomedical engineering for covid-19 pandemic: A comprehensive review. *Journal of Data Science and Intelligent Systems*, 2(4):191–204, 2024.

[28] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[29] M. Nankya, R. Chataut, and R. Akl. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. *Sensors*, 23(21):8840, 2023.

[30] S. Tariq, S. Lee, H. K. Kim, and S. S. Woo. Can-adf: The controller area network attack detection framework. *Computers & Security*, 94:101857, 2020.

[31] E. S. Hosney, I. T. A. Halim, and A. H. Yousef. An artificial intelligence approach for deploying zero trust architecture (zta). In *Proceedings of the 2022 5th International Conference on Computing and Informatics (ICCI)*, pages 343–350. IEEE, March 2022.

[32] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri. Securing the internet of things in artificial intelligence era: A comprehensive survey. *IEEE Access*, 2024.

[33] Mushtaq Al-Sharify, Talib A Al-Sharify, Noor T Al-Sharify, Zainab T Al-Sharify, Ashwaq T Al-Sharify, Mustafa Akeel Kareem, and Aymen Mohammed Khodayer Al-Dlaimi. Employing the beamforming technique to enhance the medical ambulance performance, iomt. *Tikrit Journal of Engineering Sciences*, 32(1):1–9, 2025.

[34] David Rocha, Gil Teixeira, Emanuel Vieira, João Almeida, and Joaquim Ferreira. A modular in-vehicle c-its architecture for sensor data collection, vehicular communications and cloud connectivity. *Sensors*, 23(3):1724, 2023.

[35] 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*, pages 244–259. Bentham Science Publishers, 2024.

[36] 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*, 5(3):1111–1131, 2024.

[37] M. A. Allouzi and J. Khan. Enabling zero trust security in iomt edge network. *arXiv preprint*, 2024.

[38] G. Balhareth and M. Ilyas. Optimized intrusion detection for iomt networks with tree-based machine learning and filter-based feature selection. *Sensors*, 24(17):5712, 2024.

[39] Center for Internet Security. Ddos attacks in the healthcare sector. https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector, n.d. Retrieved January 17, 2025.

[40] A. Bajwa. Ai-based emergency response systems: A systematic literature review on smart infrastructure safety. Available at SSRN, 2025. SSRN ID: 5171521.

[41] A. A. El-Saleh, A. M. Sheikh, M. A. Albreem, and M. S. Honnurvali. The internet of medical things (iomt): Opportunities and challenges. *Wireless Networks*, 31(1):327–344, 2025.

[42] Kaggle. IoT Healthcare Security Dataset. https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset, n.d. Accessed: 2025-10-26.

[43] Kaggle. Human Vital Sign Dataset. https://www.kaggle.com/datasets/nasirayub2/human-vital-sign-dataset, n.d. Accessed: 2025-10-25.

[44] Jeffrey R Suchard. Recovery from severe hyperthermia (45 c) and rhabdomyolysis induced by methamphetamine body-stuffing. *Western Journal of Emergency Medicine*, 8(3):93, 2007.