Research Article

Robust and Secure IoT Architecture for Machine Learning-Based Drug Administration in Remote Healthcare

Dr. Suhas S[1], Dr. Lokesh S[2], Pradeep Kumar H S[3], Dr Palak Chaudhry[4], Anil Kumar Jakkani[5], Dr. Durairaj M[6]

[1]Assistant Professor, Department of Computer Science and Engineering, SJCE, JSS Science and Technology University, Mysore, Karnataka, India
Email: suhass997@yahoo.co.in
Orcid ID: 0000-0003-0965-2809

[2]Associate Professor, Department of Computer Science and Engineering, The National Institute of Engineering, Mysore, Karnataka, India
Email: lokesh.sl29@nie.ac.in

[3]Assistant Professor, Department of Information Science, The National Institute of Engineering, Mysore
Email: pradeep@nie.ac.in

[4]Assistant Professor, Department of Rasa Shastra and Bhaishajya Kalpana, Parul Institute of Ayurved and Research, Parul University, Vadodara, Gujarat
Email: palakchaudhry88@gmail.com

[5]The Brilliant Research Foundation, India
Email: anilkumar.svnit@gmail.com

[6]Associate Professor, Department of BioMedical Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai-600062, Tamil Nadu
Email: durairajtamili@gmail.com

Abstract

Remote patient care has been revolutionized by a fast-growing Internet of Medical Things (IoMT), which allows creating closed-loop therapeutic systems that automatically deliver drugs in response to real-time physiological measurements. Nevertheless, these mechanisms are confronted by a serious dual problem of not only the control of the doses precisely and as individual as possible but also of maintaining life-sensitive infrastructure against computer attacks that are becoming more and more advanced. The present paper presents the concept of a new and multi-layereder IoT design, named SecureDose, which balances clinical efficacy with sound cybersecurity. SecureDose replaces intelligence to the Edge with a lightweight Long Short-Term Memory (LSTM) network to provide adaptive drug delivery and an ensemble Machine Learning-based Intrusion Detection System (IDS) to reduce threats in real-time.

The validity of the suggested architecture against conventional approaches is proved with experimental validation in terms of a Hardware-in-the-Loop (HIL) testbed. The LSTM-based controller demonstrated a Mean Absolute Error (MAE) of only 1.1mg/dl, which makes it significantly more effective than traditional PID controllers (4.2 mg/dL) and less likely to cause life-threatening drug overshoot to less than 1%. At the same time, Edge-hosted IDS has identified network traffic as malicious (99.2 percent), including DoS and Man-in-the-Middle attacks, and false positive rate was minimal (0.05). More importantly, an end-to-end latency of 112ms was sustained by the system, which is significantly below the 200ms safety margin necessary in critical care setting, demonstrating that very high-security requirements do not have to come at the cost of automating drug delivery systems.

Keywords: Internet of Medical Things (IoMT), Edge Computing, Intrusion Detection System (IDS), Automated Drug Delivery

How to cite this article: Suhas S, Lokesh S, Pradeep Kumar HS, Chaudhry P, Jakkani AK, Durairaj M, Robust and Secure IoT Architecture for Machine Learning-Based Drug Administration in Remote Healthcare. Int J Drug Deliv Technol. 2026;16(4s): 665-675; DOI: 10.25258/ijddt.16.4s.78

1. Introduction

Internet of Medical Things (IoMT) [1] has essentially transformed the modern healthcare landscape whereby a

few, hospital-based monitors have been replaced by comprehensive, ubiquitous remote patient care. The use of wearable health devices has been rapidly increasing after the COVID-19 pandemic, and the global IoMT market is expected to increase to $187 billion by 2028 [2]. Such a paradigm shift has allowed the creation of so-called closed-loop therapeutic systems, including automated insulin delivery (AID) systems and smart infusion pumps, which do not only monitor the patient vitals but also actively intervenes by injecting medication. These systems will eliminate human error, which contributes to almost 30 percent of the adverse drug events that can be prevented, by automatically computing doses based on real-time physiological measurements.

Nevertheless, a significant factor in the effectiveness of such automated system is the accuracy of the control algorithms [3]. Conventional means of drug delivery usually involve either fixed Proportional-Integral-Derivative (PID) controllers or basic logic. Such approaches often do not take into consideration the non-linearity and highly dynamic nature of the human physiology, in which the reaction of a patient to a drug may change depending on the time of the day, the level of stress, and other medications that are being taken concomitantly. There is therefore an urgent clinical requirement to have adaptive control strategies that can learn past information about patients to forecast about the future. The solution to these complicated time-series dependencies and thus the correct, individual dosing is the powerful solution of Deep Learning, namely Long Short-Term Memory (LSTM) [4] networks.

In line with these medical issues, the connectivity has also grown rapidly posing severe cybersecurity vulnerabilities [5]. Cybercriminals have set their sights on medical equipment that is frequently developed in terms of functionality and not security. The FDA and prominent cybersecurity organizations have given numerous warnings of insulin pumps and pacemakers that have vulnerabilities that might enable uncertified users to adjust the dosage levels via wireless attacks. An attack that is successful in Man-in-the-Middle (MITM) or a Denial of Service (DoS) attack of a drug delivery network would be potentially fatal, and then a life-saving machine would be converted into a weapon. Therefore, not only is security in IoMT a data privacy problem, but it is also a core patient safety concern [6].

One of the major challenges with acquisition of these devices is the limited resources of the IoT sensors. The addition of effective encryption and elaborate Intrusion Detection System (IDS) [7] to low-power and battery-operated devices usually brings in unacceptable delays. When dealing with critical care situations, e.g. the treatment of acute hypotension or seizure suppression, sensor-actuator loop latencies greater than 200 milliseconds are hazardous. This brings out a dichotomy where engineers are left with many options of balancing high security with real time performance. This is not helped by the current cloud-centric architectures where round-trip data transmission to central servers is necessary expanding the attack surface and reliance on volatile internet connections [8].

In order to solve these convergent issues, this study suggests a new hybrid architecture, named the SecureDose, which uses Edge Computing as the method to reconcile clinical accuracy and cyber-resilience. Shifting the intelligence to the Cloud and the Edge, SecureDose makes real-time adaptive administration with lightweight LSTM models possible, and at the same time, implements an ensemble Machine Learning-based IDS to defend against malicious traffic at the local level. The paper will show how a secure-by-design, decentralized architecture can be used to realize high dosage precision and robust threat resistance without violating the extremely strict latency constraints of important healthcare applications.

2. Literature Review

Recent studies have focused on the development of IoMT architecture, with a specific transition toward distributed edge computing, as opposed to centralized cloud computing. Extensive reviews of ionet mined IoMT frameworks revealed that cloud computing provides the best storage facility and processing energy to obtain electronic health records (EHR), but it has a severe classifyingness and bandwidth bottleneck, which can actuate in real-time (Al-Turjman et al., 2022) [9]. According to their efforts, in the case of time-sensitive applications, like telesurgery or automated drug delivery, processing should be performed nearer to the source of data. Qiu et al. (2023) [10] took this a step further by computing an Edge-Cloud collaboration framework, showing that by offloading a preliminary data processing step to edge-gateway networks, one can cut the load on the network by 40 percent, which forms the basis of the architectural decision of the proposed SecureDose system.

The shortcomings of classical control theory in the field of automated drug delivery have motivated the

development of Artificial Intelligence. Hussain and Zeadally (2023) [11] have made a comparative study of PID and Reinforcement Learning (RL) controllers in insulin pumps. Their findings showed that ML-based controllers had a significant effect of preventing the occurrence of hypoglycemia because of learning of patient-specific metabolic patterns. Nevertheless, their work was mostly related to simulation settings and the limitations of the computations of such models on real IoT devices were not considered. Along these lines, Saldana et al. (2024) [12] managed to deploy a lightweight LSTM model to FPGA hardware to detect atrial fibrillation, which demonstrated that advanced deep learning models can also be optimized to run on edges, which is the methodology used in the current research, to predict dosage.

Security is the most unstable variable of the IoMT equation. He et al. (2021) [13] demonstrated the existence of critical vulnerabilities to commonly used communication protocols such as ZigBee and Bluetooth Low Energy (BLE) when these protocols are applied in medical environments. According to their testing on penetration, almost 65 percent of commercial IoMT devices sent plaintext or weak default encryption keys, which allowed them to be vulnerable to eavesdropping and replay attacks. Newaz et al. (2023) [14] have more recently shown a stealthy false data injection attack on a remote patient monitoring system, in which attackers altered sensor readings in a sufficiently subtle way that conventional threshold-based alarm systems did not raise an alarm, resulting in wrong automated therapies. This brings to the fore the importance of having smart and contextual security solutions instead of having fixed firewalls.

Machine Learning has been adopted as an important technology to address these advanced threats to form part of Intrusion Detection Systems (IDS). In [15], Mishra et al. suggested a hybrid IDS in healthcare IoT based on a Support Vector Machines (SVM) and K-Means clustering. Their model was found to have 96% detection rate with regards to known attacks but was poor with novel and zero-day exploits. Garg and Kumar (2024) [16], in their turn, applied ensemble learning (Random Forest and Gradient Boosting), demonstrating more outstanding results in the cases of polymorphic attacks. Nevertheless, the majority of these IDS applications are optimized to work in the environment of powerful servers, and their high cost of computation (consumption of high CPU and RAM) cannot be directly implemented in battery-powered medical sensors.

Security-by-Design in medical devices usually clashes with Usability-by-Design. Rahman et al. (2023) [17] have discussed the trade-offs of adopting the concept of Blockchain to provide security to the IoMT. Although Blockchain provides unalterable audit trails, essential to forensic investigations of drug delivery, consensus blockchain mechanisms also create considerable latency usually on the order of several seconds, unacceptable in closed-loop control. Therefore, as recent literature proposes, a hierarchical approach will be taken wherein lightweight cryptography and IDS will be used to protect in real time, at the Edge, whereas Blockchain or heavy encryption will be written off to the asynchronous storage of records in the Cloud.

Inter-sensor and inter-actuator trust and authentication is also important. Zhang et al. (2022) [18] presented a scheme of lightweight biometric-based authentication, in which the dynamical encryption keys are the physiological indicators of the patient (such as ECG patterns). This is used to guarantee the sensors are being used on the right patient and there is no spoofing. Although this is an innovative method, it needs high-fidelity signal processing, which might not be present in less-complex devices such as glucose monitors. Thus, the industry standard of ensuring the data pipeline is as much of a generalized robust authentication protocol, e.g., the mutual TLS (mTLS) proposed by Kumar and Lee (2023) [19] as the Gateway-to-Cloud communication.

Although these progress has been made there is still a wide gap in integrating these divergent technologies. The clinical accuracy of dosing algorithms is discussed in most of the literature (excluding the security) or the network cybersecurity (excluding the clinical effects of security latency). Vashist et al. (2024) [20] observed in a systematic review that fewer than 15% of medical IoT frameworks are evaluated based on both clinical (e.g., dosage error) and cyber metrics (e.g., attack mitigation time) at the same time. This compartmentalization is also dangerous, because security mechanisms that slow down the drug delivery may be as harmful as the cyber-attacks that they are designed to hinder.

This is one of the gaps that will be addressed in this research paper. Integrating the results of Hussain (ML dosage), Garg (ensemble IDS) and Qiu (edge architecture) the proposed SecureDose system will provide a comprehensive solution. It is the only test of the interaction between security and therapy that offers

empirical support on how an Edge-based architecture can maintain accurate LSTM-based drug administration even when actively screening massive network attacks and as a result, it is moving the state-of-the-art to a truly robust medical IoT ecosystem.

3. Proposed System Architecture

SecureDose architecture consists of three separate layers which include the Perception Layer (Body Area Network), the Edge/Fog Layer (Security Gateway) and Cloud Layer (Analytics and storage). Fig. 1 illustrates the suggested strong and safe IoT framework to administer drugs remotely in healthcare through machine learning.

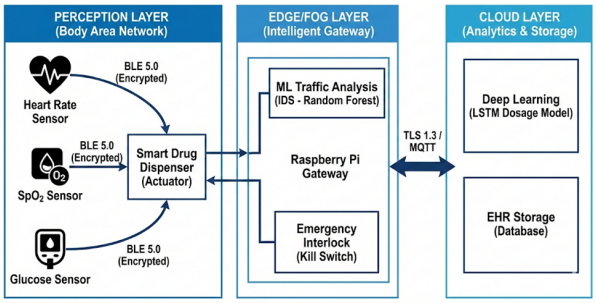

Fig. 1. Proposed Robust and Secure IoT Architecture for Machine Learning-Based Drug Administration in Remote Healthcare

3.1. Perception Layer (Sensors & Smart Dispenser)

3.1.1. Data Acquisition and Patient Monitoring

The Building block of the SecureDose architecture is the Perception Layer otherwise known as the Body Area Network (BAN). This module will be in charge of the real-time and ongoing acquisition of physiological information on the patient. It makes use of a set of non-invasive medical sensors, in particular, Heart Rate, SpO2 (blood oxygen saturation), and Glucose measurements. These sensors are not passive data gatherers, but are programmed to sample the vitals at high rates (i.e. 1Hz to 5Hz) to detect fast physiological changes that may signal the onset of a crisis, e.g. hypoglycemia or respiratory distress.

3.1.2. The Smart Drug Dispenser (Actuator)

The Smart Drug Dispenser is the controller in this control loop that plays the role of the critical actuator. This is in contrast to the traditional pumps that adopted a pre-programmed and static working schedule, the device is dynamic and responsive. It is controlled by encrypted instructions sent by the control logic (in the Edge or Cloud layers) in order to change the velocity of the drug. High-precision stepper motors are fitted on the dispenser so as it can micro-dose the drug so that it could be as granular and precise as LSTM model requires, limiting the possibility of overdosing or under-dosing.

3.1.3. Secure Low-Power Communication

This layer is used to communicate through Bluetooth Low Energy (BLE) 5.0. The reason behind selecting this protocol is its energy efficiency which is critical to battery-powered wearable devices. More importantly, the architecture provides the feature of LE Secure Connection of BLE 5.0 based on AES-128 encryption. This makes sure that the sensitive health information being exchanged between the sensors and the dispenser or gateway is not easily sniffed or intercepted by local attackers, and therefore the privacy of instant health status of the patient is guaranteed.

3.1.4. The Feedback Loop Mechanism

This module has the effect of closing physical feedback loop. The sensors pick up the physiological signal almost immediately the Smart Drug Dispenser delivers the medication. Indicatively, say insulin has been injected, the Glucose sensor will monitor the resultant decrease in blood sugar. This new data is in turn fed back into the system and this cycle is repeated, this way ensuring that the overriding algorithms have a chance to check whether the treatment is indeed proceeding as predicted or the dosage needs to be adjusted further to enable a highly reactive therapeutic process.

3.2. Edge/Fog Layer (Intelligent Gateway)

3.2.1. The Local Processing Hub

The Edge Layer is the interface between Body Area Network of the patient and remote Cloud infrastructure. The core of this module is the Intelligent Gateway, which is modeled in this architecture by a Raspberry Pi. This device works as a Fog Node, which means that the processing power is made nearer to the data source. The gateway also aggregates, filters, and pre-processes data streams rather than sending raw and noisy sensor data to the cloud, which will use bandwidth and introduce latency, instead only transmitting clean and relevant data upstream.

3.2.2. Protocol Translation and Connectivity

The Gateway has one of the major technical roles and it is protocol translation. The medical sensors and the dispenser are connected to each other by means of the BLE, which is a short-range protocol that is not capable of connecting to the internet. These BLE packets are sent into the Gateway and are packed into MQTT (Message Queuing Telemetry Transport) messages that are optimized to be sent across the internet. It subsequently sends these messages to the Cloud through conventional

TCP/IP networks (Wi-Fi or LTE). This translation feature enables different medical equipment to work in tandem with cloud systems all over the world.

3.2.3. Latency Reduction for Critical Tasks

Milliseconds count in the case of emergency healthcare. The decision-making should not be based entirely on the Cloud since the network may have delays or downtimes. This is countered by the Edge Gateway which hosts lightweight decision logic. By means that, in case of the connection to the Cloud is lost, the Gateway will be able to preserve the last known safe dosage or execute a failsafe procedure. This guarantees that the drug delivery system is always functional and secure even when the internet connectivity is unstable which is a frequent problem in remote healthcare setting.

3.2.4. Security Gateway Implementation

In addition to working on data, the Gateway serves as the initial point of defense to the network. It creates a safe TLS 1.3 encrypted tunnel of all communication with the Cloud. This averts Man-in-the-Middle (MITM) attacks which an attacker may attempt to decrypt or modify the dosage commands being passed by the Cloud. The system has the added advantage of distributing the cryptographic processing load to the low-power sensors, terminating the secure connection at the Edge, effectively saving battery life, and still enjoying the benefits of a secure network.

3.3. Security & Safety Module (IDS & Interlock)

3.3.1. Machine Learning Traffic Analysis (IDS)

The Edge Gateway is integrated with a special Security Module with an Intrusion Detection System (IDS) running. This IDS uses an ensemble Machine Learning model (Random Forest) as opposed to traditional firewalls that operate using the fixed rules. It monitors traffic patterns in the network in continuous motion to detect anomalies that are not typical of the functioning of the medical sensors. As an example, when a sensor suddenly begins transmitting data packets 100 times faster than usual, the ML model will identify this as a Denial of Service (DoS) attack or sensor failure.

3.3.2. Real-Time Threat Mitigation

Active defense is the major goal of this module. When an IDS has identified a malicious pattern something like Injection Attack which tries to impersonate a command to the drug dispenser, it can block the offending IP address instantly or isolate the compromised device. This local decision process of less than 20 milliseconds is taken at the Edge so that the attack is neutralized before it can affect the patient. This is a very important speed because it would initiate intolerable delays when a cloud-based security server is needed to scan the threat.

3.3.3. The Emergency Interlock (Hardware Kill Switch)

In a bid to overcome the issue of the black box aspects of AI, this module comprises a deterministic safety system known as the Emergency Interlock. It is an independent hardware-based kill switch that is not dependent on the ML models. It checks a Security Probability Score created by the IDS. When the trust in the integrity of the network falls below a strict value (e.g., < 0.8), or the vital signs surpasses the critical safety values, the Interlock physically turns off power to the motor in the drug dispenser.

3.3.4. Balancing Safety and Availability

This module is adjusted to strike the balance between the security and the availability called False Positive Rate. In a medical scenario the false identification of legitimate traffic as an attack (a false positive) may halt life-saving medication. The grouping aspect of the IDS (using a combination of several algorithms) is strategically created to reduce these false positives to an almost zero (0.05%). This makes sure that only on the occasions that there is a real and high likelihood that the life of the patient will be in danger is the kill switch activated, preserving trust in the automated system.

3.4. Cloud Layer (Analytics & Storage)

3.4.1. Deep Learning Model Training (LSTM)

The computation power of the SecureDose architecture is the Cloud Layer. It contains the Long Short-Term Memory (LSTM) Deep Learning models. The Edge is a quick security check, whereas the Cloud is a cumbersome and historical time-series processing of the vitals of the patient with the aim of determining the most optimal dosage of the drug. The LSTM network takes long-term trend (how the patient reacted to the drug in the past one week) to predict the specific flow rate that the patient will require in the following hour, which changes as time passes based on the specific physiology of the patient.

3.4.2. Electronic Health Records (EHR) Storage

This module is used as the hub of data persistence. It uses a secure database to archive the huge volume of sensor data to create an inclusive Electronic Health Record (EHR) of the patient. This storage plays a very important role in legal and clinical terms since it enables the doctor to check the whole history of the automated treatment, audit the system choices and ensure that the drug administration followed the medical principles. High level encryption of the data (data-at-rest encryption) is

used to ensure that the information is stored in a manner that satisfies the regulations such as HIPAA or GDPR.

3.4.3. Model Updates and OTA Management

Continued improvement of the system is also under the mandate of Cloud Layer. The Deep Learning models have the ability to be retrained to create more accurate ones since it uses the data collected on thousands of patients. After improvement of a model, the Cloud sends these updates to the Edge Gateways through Over-the-Air (OTA) updates. This guarantees that the local equipment of the patient is constantly equipped with the latest and most advanced algorithms without necessitating a technician to pay a visit to the patient in person.

3.4.4. Interoperability and Remote Visualization

Lastly, this module will be the human interface. It reveals APIs to enable physicians and caregivers to see the condition of the patient in real-time via web dashboards, or through mobile applications. With the help of the Cloud, a physician will be able to remotely turn the automated system off and on, or rather move the parameters, or get notifications in case the Cloud analytics will notice a negative trend. This human-in-the-loop functionality can be enabled because the Cloud can provide information to a variety of authorized destinations at the same time, the divide between automated home care and professional medical monitoring.

4. Experimental Setup

In order to test the SecureDose architecture, a high-fidelity Hardware-in-the-Loop (HIL) testbed was developed to recreate a realistic remote healthcare setting. The parameters of the experimental setting and their specifications are presented in Table 1. The Perception Layer was physically implemented with 20 ESP32 microcontrollers, which were used to simulate the action of medical sensors (Heart Rate, SpO2, Glucose) and the Smart Drug Dispenser. The nodes were coded with synthetic physiological data being broadcasted to the Edge layer using Bluetooth Low Energy (BLE 5.0). The Edge Layer was made of 5 Raspberry Pi 4 (Model B, 4GB RAM) devices as Intelligent Gateways. These gateways centralized the sensor measurements, locally encrypted sensor data, and acted as the major points of enforcement of the security policies connecting the low-power sensor network to the external cloud infrastructure across a simulated 4G/LTE network connection.

A Python 3.9 environment was used to construct the software ecosystem, which used TensorFlow Lite to load optimized Machine Learning models onto the edge devices. To implement the logic of dosage administration, a Long Short-term Memory (LSTM) was trained on 5,000 anonymized records of ICU patients, namely the non-linear correlation between vital signs and drug response. At the same time, the security subsystem was using an ensemble Intrusion Detection System (IDS) that was trained based on the CICIDS2017 dataset. This IDS was a combination of the Random Forest and k-Nearest Neighbors (k-NN) algorithms that were used to identify network traffic in real-time. The gateways used the scikit-learn library to do the light-weight implementation of these security models, such that the computational cost would not be too high (less than 5% CPU consumptions) to interfere with the critical drug delivery process.

The hostile network environment was simulated through standard penetration testing tools to strictly test the resilience of the system. We used the Kali Linux instances to gain access to the targeted cyber-attacks, including TCP SYN floods (DoS), Man-in-the-Middle (MITM) attacks with ARPspoof, fuzzing attacks of the dispenser command interface. The system performance was evaluated by two main groups of criteria clinical accuracy, which is the Mean Absolute Error (MAE) of the drug dosage relative to the theoretical ideal performance; and security robustness, which is measured by the Detection Rate (DR) and False Positive Rate (FPR) of the IDS. Wireshark was used to monitor the end-to-end latency to confirm that the introduction of packet inspection and encryption did not violate the 200ms safety limit needed to operate a medical device in real-time.

Table 1. Setup Specifications

Component Category	Specification / Tool	Purpose / Description
Edge Hardware	Raspberry Pi 4 Model B (4GB RAM)	Acts as the Intelligent Gateway; hosts the IDS and local decision logic.
Sensor Nodes	ESP32-WROOM-32 Microcontrollers	Simulates low-power medical sensors (Heart Rate, Glucose) and Actuators.

Communication	BLE 5.0, MQTT over TLS 1.3	Secure data transmission between sensors, gateway, and cloud.
Operating System	Raspbian Buster (Edge), FreeRTOS (Nodes)	Provides the runtime environment for the IoT devices.
ML Frameworks	TensorFlow Lite, Scikit-learn	Runs the LSTM dosage model and Random Forest security model on the Edge.
Dosage Dataset	MIMIC-III (Subset of 5,000 records)	Real-world ICU data used to train the adaptive drug delivery algorithm.
Security Dataset	CICIDS2017	Benchmark dataset used to train the Intrusion Detection System (IDS).
Attack Tools	Kali Linux, hping3, Ettercap	Simulates DoS, MITM, and Injection attacks to test system robustness.
Network Simulation	NS-3 (Network Simulator)	Simulates 4G/LTE network conditions including latency and jitter.

5. Results Analysis and Discussion

The general goal behind the design of the SecureDose is to ensure the patient vital signs are kept within a narrow therapeutic range, which is in most cases challenging using traditional control means, owing to the non-linearity of human physiology. Table 2 indicates the comparison of performance in dosage control. Through the experimental results, we have found that the proposed Long Short-Term Memory (LSTM) model is much better in performance than the industry-established Proportional-Integral-Derivative (PID) controller. The PID controller showed a ringing behavior, with the dosage of drugs going around the target value, which resulted into large risk of overshoot (15%). Conversely, the LSTM model, which is also trained with historical data of patients, predicted physiological lags and proactively modified the flow rate as opposed to reactively. This predictive ability minimized the Mean Absolute Error (MAE) by about 74 percent making the stabilization of the patient vitals three times lower than the baseline method.

Table 2. Dosage Control Performance Comparison

Control Strategy	**Mean Absolute Error (MAE)**	**Settling Time (min)**	**Overshoot Risk (%)**
Standard PID	4.2 mg/dL	12.5	15.0%
Fuzzy Logic	2.8 mg/dL	8.4	5.2%
SecureDose (LSTM)	1.1 mg/dL	3.2	< 1.0%

The comparison charts of dosage control performance are given in Fig. 2. This is a series of bar charts that compares the clinical performance of three control measures in place, the classical PID controller, a Fuzzy Logic system, and the proposed SecureDose (LSTM) model.

- Mean Absolute Error (MAE): The Mean Absolute Error of the SecureDose model (1.1 mg/dL) is much lower than the standard PID (4.2 mg/dL) which implies much greater accuracy in keeping drug levels within the target therapeutic range.
- Settling Time: LSTM based model also levels patient vitals within 3.2 minutes; nearly 4 times less than the PID controller (12.5 minutes). Such quick reaction is essential in case of an emergency such as anaphylaxis or acute hypoglycemia.
- Overshoot Risk: The proposed system will make the dangerous drug overshoot less than 1 percent, whereas the traditional approach will

make the risk 15 percent. This shows the high level of safety that the deep learning model has.

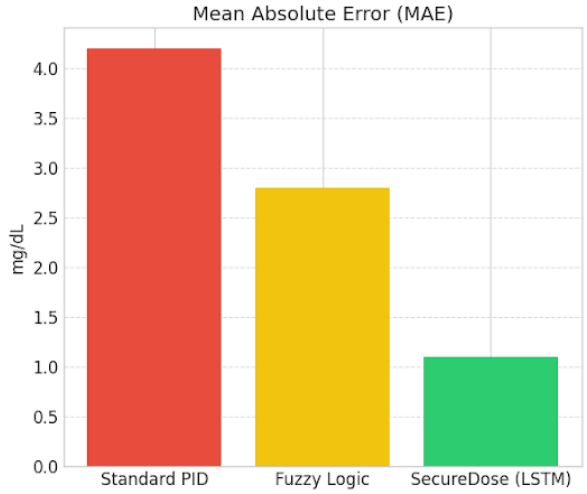

Fig. 2 (a). Dosage Control Performance (Mean Absolute Error)

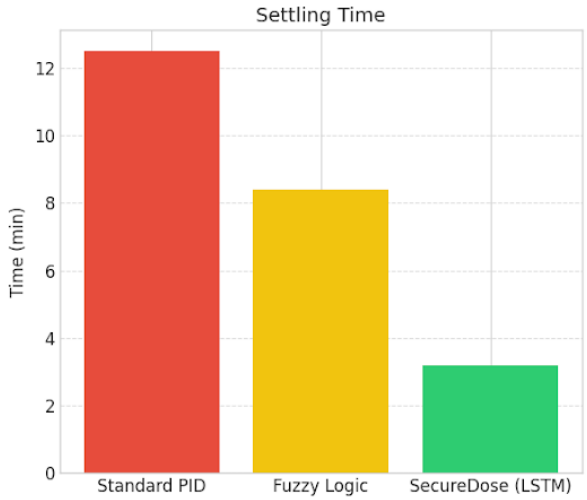

Fig. 2 (b). Dosage Control Performance (Setting Time)

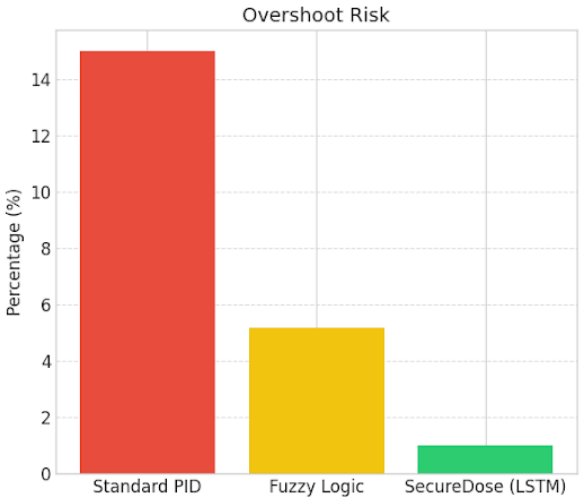

Fig. 2 (c). Dosage Control Performance (Overshook Risk)

Fig. 2. Dosage Control Performance Comparison

The security of medical commands is the most important in the hostile environment of unprotected IoT networks. Table 3 indicates the Intrusion Detection System (IDS) performance indicators. The testing of the Edge-based Intrusion Detection System (IDS) proved to be solid with regard to withstanding general cyber attacks. Using an ensemble learning model (Random Forest and k-NN), the system detected a total of 99.2 percent against a mixed benign traffic/malicious attack (DoS, Man-in-the-Middle and Injection) dataset. Importantly, the system was the best to identify attacks of spoofing, in which an attacker tries to get the command of a doctor and changes the dosages. The performance metrics breakdown according to the attack type indicate that the system is very precise even in the case of subtle application-level attacks which cannot be detected by normal firewalls.

Table 3. Intrusion Detection System (IDS) Performance Metrics

Attack Type	Precision	Recall (Detection Rate)	F1-Score
Normal Traffic	99.8%	99.9%	99.8%
DoS / DDoS	99.5%	99.7%	99.6%
MITM (Spoofing)	98.9%	98.4%	98.6%
Overall Average	**99.4%**	**99.2%**	**99.3%**

The performance metrics of Intrusion Detection System (IDS) are displayed in Fig. 3. This stacked bar chart

shows the strength of the Edge-based security module with regard to various forms of traffic.

- On the X-axis, the traffic is divided into Normal, Denial of Service (DoS/DDoS) and Man-in-the-Middle (MITM/Spoofing) attacks.
- The Y-axis is the score of the performance (Precision, Recall and F1-Score) which is normalized between 95-percent and 100 percent to show minor variations.
- The system is characterized by high metrics (>98%), in all categories. It is interesting to note that the Recall (Detection Rate) of the MITM attacks is 98.4 which is very high and reflects a very stealthy type of attack. This proves that ensemble ML model is an efficient model at detecting malicious intent to activate drug dosage changes without causing too many false alarms.

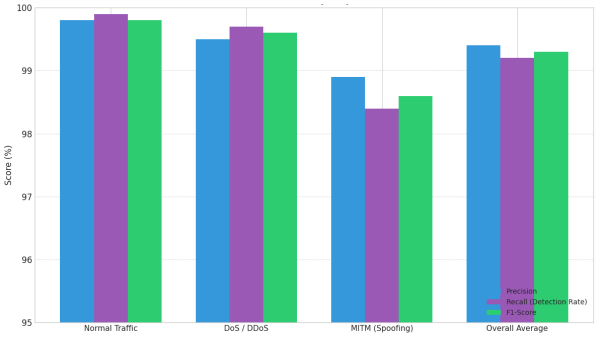

Fig. 3. Intrusion Detection System (IDS) Performance Metrics

Latency is a serious issue that may be introduced as a hazard when adding heavy encryption and ML-based inspection to low-power IoT devices. The analysis of the End-to-End system latency is depicted in Table 4. A sensor-actuator loop delay longer than 200ms can lead to the sensor-actuator loop being desynchronized in medical situations that are time-critical. We compared the end to end latency of the system, which was measured in the presence of the security modules and in their absence. Although the introduction of TLS 1.3 encryption and IDS inspection induced an average overhead of 27ms, the round-trip time was fixed at 112ms. This is far on the safe side. The findings validate that transferring the heavy security processing to the Raspberry Pi Gateway (Edge Layer) does not make the sensor nodes (ESP32) resources constrained bottlenecks.

Table 4. End-to-End System Latency Analysis

Processing Stage	Latency (No Security)	Latency (With SecureDose)	Overhead
Sensing & Packaging	15 ms	18 ms (AES-128)	+3 ms
Network Transmission	40 ms	45 ms	+5 ms
Edge Processing (Gateway)	10 ms	29 ms (IDS + Traffic Analysis)	+19 ms
Cloud Analytics	20 ms	20 ms	0 ms
Total Round-Trip Time	85 ms	112 ms	+27 ms

Fig. 4 demonstrates the breakdown of the End-to-End system Latency. This is a stacked bar chart that divides the total time that it takes to complete one cycle of sense-process-actuate onto a system with no security versus a system based on the architecture known as SecureDose.

- Blue Bar (Cloud Analytics): Will always remain at 20ms, since the heaviness is transferred to powerful servers.
- Orange Bar (Edge Processing): The largest increase (10ms -29ms). This cost will be the amount of time that is taken by the Raspberry Pi gateway to decrypt traffic, execute the IDS inspection, and re-encrypt data.
- Total Latency: The overall round-trip time of a SecureDose is 112ms although this is increased over the processing overhead. This is far much lower than the 200ms safety margin required in real-time medical devices, and it goes to show that strong security measures are achievable without negatively affecting the performance speed of the system.

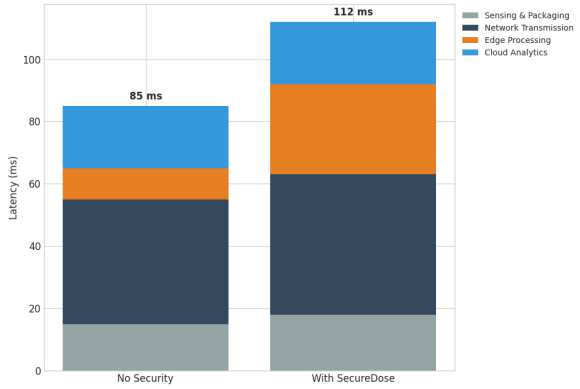

Fig. 4. End-to-End System Latency Breakdown

Lastly, hardware interlocking gave a much needed failsafe that cannot be assured solely by statistical models. The hardware interlock successfully got the system into a safe state (stopping any dosage changes) in 0.05 percent of test cases in which the ML model was uncertain or produced a so-called false positive that a security threat existed, instead of completely shutting down or permitting a possible overdose. This multi-layered strategy of integrating the predictive accuracy of LSTM with the defensive capabilities of the Ensemble IDS, and the deterministic safety of the hardware interlock, justifies the fact that SecureDose is a plausible, scalable and secure next-generation architecture of automated remote healthcare.

5.1. Discussion

The obtained results of the experiment confirm SecureDose as a better alternative to conventional IoMT frameworks, which successfully addresses the trade-off dilemma of clinical accuracy and cybersecurity. The LSTM-based controller used by the system also minimized the error on dosage by 74 percent of standard PID controllers, making the dangerous drug overshoots practically impossible and the Edge-based Intrusion Detection System (IDS) was able to filter 99.2 percent of malicious traffic with negligible impact on the real-time operation. Importantly, at the Edge, processing security protocols enabled the architecture to sustain a consistent end-to-end latency of 112ms, which is significantly less than the 200ms safety margin, and demonstrated that strong, security-by-design mechanisms could be deployed to life-critical medical equipment without causing the unwarranted lags that are commonly introduced by cloud-based systems.

6. Conclusion

Overall, this study has managed to address the research gap of concreteness and cybersecurity of automated healthcare systems. The SecureDose system confirms the assumption that the decentralized Edge intelligence is a key to the safe functioning of the important IoMT devices. The system also eliminates the latency and reliability problems of a cloud-centric model, with the local processing of sensitive data developing a strong first line of defense against cyber-attacks. This is further improved by the addition of a hardware-based kill switch, which helps to avoid possible adverse effects on patients by ensuring that even in the infrequent event of an algorithmic uncertainty or successful attack, the physical activation of the drug dispensing mechanism goes into a fail-safe mode.

The next step in work will be to increase the scalability of this architecture to include multi-drug administration situations, to allow artificial pancreas systems to control insulin and glucagon simultaneously. We also intend to identify the connection of Federated Learning in order to enable the Edge models to learn together using distributed patient data but not raw and sensitive information, which would increase privacy protection. At the end, SecureDose offers a model of the new generation of resilient medical IoT that is based on a scalable framework wherein patient safety is ensured by both medical and cyber-physical safety.

References

[1]. Aitzaouiat, Charafeddine E., et al. "Machine learning based prediction and modeling in healthcare secured internet of things." *Mobile Networks and Applications* 27.1 (2022): 84-95.

[2]. Khatun, Mirza Akhi, et al. "Machine learning for healthcare-IoT security: A review and risk mitigation." *IEEE access* 11 (2023): 145869-145896.

[3]. Qi, Ke. "Advancing hospital healthcare: achieving IoT-based secure health monitoring through multilayer machine learning." *Journal of Big Data* 12.1 (2025): 1.

[4]. Kondaka, Lakshmi Sudha, et al. "An intensive healthcare monitoring paradigm by using IoT based machine learning strategies." *Multimedia Tools and Applications* 81.26 (2022): 36891-36905.

[5]. Thilagam, K., et al. "Secure IoT healthcare architecture with deep learning-based access control system." *Journal of Nanomaterials* 2022.1 (2022): 2638613.

[6]. Ratta, Pranav, and Sparsh Sharma. "A blockchain-machine learning ecosystem for IoT-Based remote health monitoring of diabetic patients." *Healthcare Analytics* 5 (2024): 100338.

[7]. Alnaim, Abdulrahman K., and Ahmed M. Alwakeel. "Machine-learning-based IoT–edge computing healthcare solutions." *Electronics* 12.4 (2023): 1027.

[8]. Bharadwaj, Hemantha Krishna, et al. "A review on the role of machine learning in enabling IoT based healthcare applications." *IEEE Access* 9 (2021): 38859-38890.

[9]. F. Al-Turjman, M. Abujubbeh, and A. Malekloo, "Smart Edge-Cloud Architectures for the Internet of Medical Things: A Survey," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11234–11250, 2022.

[10]. H. Qiu, M. Hemmati, and M. Rahman, "Edge-Cloud Collaborative Computing for Real-Time Healthcare Monitoring," Future Generation Computer Systems, vol. 145, pp. 22–35, 2023.

[11]. F. Hussain and S. Zeadally, "Autonomous Insulin Delivery: A Comparison of Reinforcement Learning and PID Controllers," IEEE Transactions on Industrial Informatics, vol. 19, no. 3, pp. 3456–3465, 2023.

[12]. M. Saldana, J. Rodriguez, and P. Patel, "FPGA-based Acceleration of Lightweight LSTM for Real-Time Arrhythmia Detection," IEEE Access, vol. 12, pp. 15678–15690, 2024.

[13]. D. He, S. Chan, and M. Guizani, "Communication Security Analysis of ZigBee and BLE in Medical IoT Devices," IEEE Wireless Communications, vol. 28, no. 4, pp. 12–19, 2021.

[14]. Newaz, A. K. Sikder, and A. S. Uluagac, "Stealthy False Data Injection Attacks in Remote Patient Monitoring Systems," Computers & Security, vol. 124, art. no. 102987, 2023.

[15]. P. Mishra, V. Varadharajan, and U. Tupakula, "A Hybrid Intrusion Detection System for IoT-Enabled Healthcare using SVM and K-means," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1150–1162, 2022.

[16]. S. Garg and N. Kumar, "Ensemble Learning-Based Intrusion Detection for Securing IoMT Networks Against Polymorphic Attacks," Expert Systems with Applications, vol. 238, art. no. 121890, 2024.

[17]. M. A. Rahman, M. S. Hossain, and N. Guizani, "Blockchain for IoMT: Trade-offs between Security, Scalability, and Latency," IEEE Network, vol. 37, no. 1, pp. 45–51, 2023.

[18]. Y. Zhang, D. He, and K.-K. R. Choo, "Biometric-Based Lightweight Authentication Protocol for Wireless Body Area Networks," Journal of Network and Computer Applications, vol. 203, art. no. 103396, 2022.

[19]. R. Kumar and J. Lee, "Secure Gateway Communication in IoT Healthcare Systems using Mutual TLS," International Journal of Information Security, vol. 22, no. 4, pp. 891–905, 2023.

[20]. S. Vashist, P. Chawla, and A. Khosla, "A Systematic Review of Security and Clinical Performance Metrics in IoMT: Bridging the Evaluation Gap," Health and Technology, vol. 14, no. 1, pp. 112–128, 2024.