Securing Internet of Medical Things: An Advanced Federated Learning Approach

Anass Misbah[1], Anass Sebbar[2], Imad Hafidi[3]
Computer Science and Mathematics Lab, National School of Applied Sciences, Khouribga, Morocco[1]
Computer Science and Mathematics Lab, University International of Rabat, Rabat, Morocco[2]
Computer Science and Mathematics Lab, Sultan Moulay Slimane University, Beni Mellal, Morocco[3]

Abstract—**The Internet of Medical Things (IoMT) is transforming healthcare through extensive automation, data collection, and real-time communication among interconnected devices. However, this rapid expansion introduces significant security vulnerabilities that traditional centralized solutions or device-level protections often fail to adequately address due to challenges related to latency, scalability, and resource constraints. This study presents a novel federated learning (FL) framework tailored for IoMT security, incorporating techniques such as stacking, federated dynamic averaging, and active user participation to decentralize and enhance attack classification at the edge. Utilizing the CICIoMT2024 dataset, which encompasses 18 attack classes and 45 features, we deploy Random Forest (RF), AdaBoost, Support Vector Machine (SVM), and Deep Learning (DL) models across 10 simulated edge devices. Our federated approach effectively distributes computational loads, mitigating the strain on central servers and individual devices, thereby enhancing adaptability and resource efficiency within IoMT networks. The RF model achieves the highest accuracy of 99.22%, closely followed by AdaBoost, demonstrating the feasibility of FL for robust and scalable edge security. While this study validates the proposed framework using a single realistic dataset in a controlled environment, future work will explore additional datasets and real-world scenarios to further substantiate the generalization and effectiveness of the approach. This research underscores the potential of federated learning to address the unique security and computational constraints of IoMT, paving the way for practical, decentralized deployments that strengthen device-level defenses across diverse healthcare settings.**

***Keywords*—Internet of Medical Things (IoMT); federated learning; machine learning; security; intrusion detection systems; decentralized framework**

I. Introduction

The integration of medical devices within healthcare systems, known as the Internet of Medical Things (IoMT) [1], is rapidly transforming patient care by connecting devices and applications that communicate with healthcare IT networks. This interconnected framework enhances service delivery but simultaneously raises significant security challenges, particularly concerning the protection of sensitive medical data. Unlike other constrained environments, IoMT devices operate within highly regulated healthcare settings where data privacy and real-time responsiveness are critical. Traditional centralized machine learning models are often unsuitable for IoMT applications due to stringent data privacy regulations and the necessity for efficient, localized computation.

Addressing these challenges, this study introduces a novel framework employing Federated Learning (FL) [2] and Lightweight Machine Learning (LML) [3] to enhance security while accommodating the computational limitations inherent in IoMT devices. In IoMT systems, connected medical devices gather and exchange information with healthcare infrastructure, creating a network where security and privacy are paramount [4]. Unlike centralized learning models, FL offers a decentralized approach that trains models on local data without transferring sensitive information to a central server, thereby reducing privacy risks [5]. FL is particularly advantageous for IoMT, enabling secure and private model training at the edge for applications such as patient outcome prediction and resource management [6].

However, applying FL in IoMT contexts presents unique challenges that are distinct from other constrained device scenarios. These include heterogeneous device data, non-identically distributed (Non-IID) data, limited device resources, and the complexity of securely aggregating model updates [7]. Unlike industrial IoT or consumer IoT devices, IoMT devices often handle highly sensitive and regulated data, necessitating more robust privacy-preserving mechanisms and compliance with healthcare standards. This research aims to address these IoMT-specific challenges through three advanced FL techniques—stacking, federated dynamic averaging, and active user participation—designed to improve attack detection accuracy and computational efficiency at the edge level.

The study leverages the CICIoMT2024 dataset [8], which encompasses 18 distinct attack classes and 45 features, to evaluate the effectiveness of various machine learning models, including Random Forest (RF), AdaBoost, Support Vector Machine (SVM), and Deep Learning (DL), deployed across 10 simulated edge devices. Preliminary results indicate that ensemble models, particularly Random Forest and AdaBoost, exhibit superior performance. The Random Forest model achieved an accuracy of 99.22%, precision of 99.38%, recall of 99.22%, and an F1 score of 99.09%, while AdaBoost demonstrated an accuracy of 98.59%, precision of 98.84%, recall of 98.59%, and an F1 score of 98.22%. In contrast, the Deep Learning and Support Vector Machine models attained lower accuracies of 77.59% and 65.70%, respectively.

This study contributes to IoMT security by:

1) Developing and tailoring federated learning models for IoMT: This research introduces FL models specifically adapted to address the unique security and computational constraints of IoMT devices. These adaptations enable effective deployment in resource-limited environments while maintaining high model performance and efficiency.

2) Enhancing privacy and anomaly detection in IoMT systems: By leveraging privacy-preserving techniques and robust anomaly detection methods, this study strengthens IoMT security. It safeguards patient data and provides early detection of potential threats, thereby enhancing the resilience of IoMT ecosystems.

3) Validating on realistic, open datasets in controlled testbed environments: Utilizing the CICIoMT2024 dataset within a structured testbed environment ensures that the proposed solutions are practically applicable and reliable. This approach reflects real-world IoMT scenarios, thereby enhancing the relevance and scalability of the findings.

The paper is organized as follows: Section II reviews current methodologies for securing IoMT, emphasizing FL-based solutions and providing a dataset benchmark. Section III identifies research gaps and presents motivations for this study. Section IV details the proposed approach and experimental findings. Finally, Section V concludes the study, offering perspectives on future research directions. Table I lists abbreviations used throughout the paper.

TABLE I. ABBREVIATIONS AND THEIR MEANINGS

Abbreviation	Definition
IoMT	Internet of Medical Things
FL	Federated Learning
LML	Lightweight Machine Learning
RF	Random Forest
SVM	Support Vector Machine
DL	Deep Learning
IDS	Intrusion Detection System
MQTT	Message Queuing Telemetry Transport
DoS	Denial of Service
DDoS	Distributed Denial of Service
FDA	Federated Dynamic Averaging
PFL	Personalized Federated Learning
FU	Federated Unlearning
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
BLE	Bluetooth Low Energy
SDN	Software-Defined Networking
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IGMP	Internet Group Management Protocol
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
DNS	Domain Name System
SSH	Secure Shell
SMTP	Simple Mail Transfer Protocol
IRC	Internet Relay Chat
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
LLC	Logical Link Control
RBF	Radial Basis Function
Non-IID	Non-Independent and Identically Distributed

II. RELATED WORK

A. Security Challenges of IoMT

Recent surveys on security in the Internet of Medical Things (IoMT) have highlighted key challenges and trends in securing healthcare systems and devices. A study by [9] surveyed healthcare organizations and found that most respondents identified data privacy and security as their top concerns, with vulnerabilities in medical devices being a significant worry. Similarly, [10] focused on healthcare professionals' perceptions of IoMT security and discovered that while there is growing awareness of security risks, many professionals lack sufficient training and resources to address these issues effectively. In contrast, [11] examined security practices among IoMT device manufacturers and uncovered a lack of standardized security protocols and insufficient investment in security measures during the development phase. Additionally, [12] analyzed the impact of regulatory frameworks on IoMT security, revealing inconsistencies in compliance requirements across different regions and highlighting the need for harmonization to ensure comprehensive security standards.

The surveys summarized in Table II underscore the complex landscape of IoMT security, emphasizing the necessity for robust security strategies, increased awareness, and collaborative efforts among stakeholders to effectively counter emerging threats.

B. Federated Learning with IoMT

Recent contributions summarized in Table III demonstrate promising advancements in applying federated learning (FL) to secure the Internet of Medical Things (IoMT). The work of [23] proposed a federated learning approach to improve intrusion detection accuracy in IoMT networks. Also, [24] developed a federated learning model for malware detection on IoMT devices with minimal data sharing. In addition, [25] introduced a privacy-preserving federated learning framework for collaborative analysis of medical data from diverse sources. Moreover, [26] presented a federated learning-based anomaly detection system to enhance security in IoMT by detecting unusual patterns in medical sensor data [27]-[30].

Related surveys and research works see Table IV.

C. Open Datasets for IoMT Security

Recent advancements in cybersecurity research have led to the development of several comprehensive datasets (as illustrated in **Table V**) tailored for specific applications within the Internet of Medical Things (IoMT) and broader network security domains. The work of [36] introduced a dynamic dataset focusing on ransomware detection and mitigation in integrated clinical environments, emphasizing the need for intelligent security solutions in healthcare settings. Furthermore, [37] and [38] provided a dataset for effective attack detection in IoMT smart environments using deep belief neural networks, highlighting the increasing complexity and variety of threats in medical IoT networks.

The HIIDS dataset, developed by [39], introduces a hybrid intelligent intrusion detection system that integrates machine learning and metaheuristic algorithms to enhance security in IoT-based healthcare applications. Similarly, [40] conducted a comparative analysis of various machine learning techniques for intrusion detection in smart healthcare systems, presenting a dataset that facilitates the evaluation of different methodologies in this critical area.

Focusing on secure wireless communications, [41] proposed a novel approach to ensuring secure Bluetooth communication in smart healthcare systems, accompanied by a community dataset and an intrusion detection system. Meanwhile, [42] introduced a security model leveraging LightGBM and transformer technologies to safeguard healthcare systems

TABLE II. Overview of Attack Types and Risks in IoT Medical Devices. This Table Summarizes Various Attack Types, their Risk Levels, and the Affected Devices within the Domain of IoT Medical Devices, along with Relevant Academic References for Further Reading

Attack Description	Attack Type	Risk Level	Attack Class	Affected Devices	Domain	Academic Reference
Eavesdropping	Passive Attack	Moderate	Data Breach	IoT Medical Devices	Network/Comm.	[13]
Device Tampering	Active Attack	High	Physical	IoT Medical Devices	Device Security	[14]
Data Modification	Active Attack	High	Data Breach	IoT Medical Devices	Data Security	[15]
Denial of Service (DoS)	Active Attack	High	Availability	IoT Medical Devices	Network/Comm.	[16]
Man-in-the-Middle (MitM)	Active Attack	High	MITM	IoT Medical Devices	Network/Comm.	[17]
Replay Attacks	Active Attack	Moderate	Replay	IoT Medical Devices	Network/Comm.	[18]
Insider Attacks	Active Attack	High	Insider	IoT Medical Devices	Device Security	[19]
Malware Infection	Active Attack	High	Malware	IoT Medical Devices	Software Security	[12]
Password Cracking	Active Attack	Moderate	Password	IoT Medical Devices	Authentication	[20]
Wireless Attacks (e.g., rogue AP)	Active Attack	High	Wireless	IoT Medical Devices	Network/Comm.	[21]
Social Engineering	Active Attack	Moderate	Social	IoT Medical Devices	Human Factors	[22]

TABLE III. Recent Contributions of Federated Learning in Securing IoMT

Reference	Application	Key Findings	Performance Metrics
[23]	Intrusion Detection	Federated learning approach improves intrusion detection accuracy in IoMT networks.	Detection accuracy: 95%, False positive rate: 2%
[24]	Malware Detection	Federated learning model effectively detects malware on IoMT devices with minimal data sharing.	Detection accuracy: 93%, Latency: 150ms
[25]	Privacy-Preserving Data Analysis	Federated learning preserves patient privacy while enabling collaborative medical data analysis from diverse sources.	Privacy loss: <1%, Data utility: 85%
[26]	Anomaly Detection	Federated learning-based anomaly detection system enhances security in IoMT by detecting unusual patterns in medical sensor data.	Detection accuracy: 92%, Precision: 90%

from cyberattacks, offering a dataset that supports the application of advanced machine learning techniques in healthcare cybersecurity.

Additionally, the CICIoMT2024 dataset [8] addresses the growing need for securing IoMT devices in healthcare by capturing interactions over multiple protocols (HTTP, MQTT, CoAP, Bluetooth) and simulating various attack vectors. This comprehensive data source facilitates the development of robust security measures tailored to healthcare IoMT environments. Together, these datasets significantly contribute to the field by enabling the development and testing of effective security solutions to safeguard healthcare infrastructure against an evolving threat landscape.

The primary aim of CICIoMT2024 is to propose a comprehensive benchmark dataset that enables the development and evaluation of security solutions for the Internet of Medical Things (IoMT). To achieve this, 18 types of attacks were executed on an IoMT testbed comprising 40 devices, including 25 real devices and 15 simulated ones. This testbed was configured to simulate diverse protocols utilized in healthcare settings, such as Wi-Fi, MQTT, and Bluetooth.

These attacks were systematically categorized into five classes: Distributed Denial of Service (DDoS), Denial of Service (DoS), Reconnaissance (Recon), MQTT-specific attacks, and spoofing. The objective is to establish a foundational benchmark that complements existing state-of-the-art contributions in the field. Through this initiative, researchers are provided with a valuable resource for exploring and developing new security solutions tailored to the unique challenges of healthcare systems, including advanced machine learning techniques.

Significantly, the research extends beyond the mere execution of attacks on IoMT devices. It also captures the lifecycle of these devices across various critical phases, from their initial network integration to eventual disconnection. This process, known as profiling, allows classifiers to detect anomalies

TABLE IV. COMPARATIVE SUMMARY OF RELATED SURVEYS AND RESEARCH WORKS

Article	Focus	Key Contributions
Enhancing Internet of Medical Things Security with AI [1]	AI for IoMT security	Reviews AI models for threat detection in IoMT, discussing anomaly detection, pattern recognition, and predictive analytics.
Federated Learning for IoMT [5]	Federated learning in IoMT	Explores federated learning algorithms, data heterogeneity, privacy, and communication protocols in IoMT.
AI for IoMT Security with Cloud–Fog–Edge [31]	AI-driven IDS in IoMT	Covers AI-driven intrusion detection systems for real-time threat detection and integration of Cloud, Fog, and Edge computing for enhanced IoMT security.
Privacy-preserving Federated Learning with Edge [7]	Privacy in federated learning	Proposes privacy-preserving federated learning with edge computing for secure and efficient data aggregation in IoMT environments.
Fed-Inforce-Fusion: Federated Reinforcement Model [32]	Federated reinforcement learning	Combines federated and reinforcement learning to develop dynamic defense and attack mitigation strategies in IoMT.
FedDICE for Ransomware Detection [33]	Ransomware in clinical IoMT	Introduces an SDN-based model for ransomware detection and isolation, enhancing resilience and privacy in clinical IoMT environments.
Federated Learning in Medical Applications [34]	Federated learning in healthcare	Provides a taxonomy of federated learning applications in healthcare, focusing on privacy preservation, communication efficiency, and resource optimization.
OpenFL: Open-Source Federated Framework [35]	Open-source federated learning	Describes the OpenFL framework, which supports diverse data types and models while ensuring privacy, and discusses its real-world applications in IoMT.

TABLE V. COMPARISON OF DIFFERENT CYBERSECURITY DATASETS (ACCURACIES BASED ON [31], [8])

Dataset	Focus	Content	Applications	Unique Features	Accuracy
ICE [36]	ICS security	Industrial protocol traffic (Modbus, DNP3)	ICS-specific IDS, anomaly detection	Focus on industrial protocols	97% - 100%
CIC-IDS-2017 [37], [38]	Network intrusion	Various attack scenarios	IDS, ML training	Comprehensive labeled data	96% - 98%
NSL-KDD [46], [39]	Network intrusion	Traffic data with attack types (DoS, R2L, U2R, probing)	IDS benchmarking	Balanced distribution, updated version	86% - 96%
UNSW-NB15 [47], [40]	Modern network intrusion	Contemporary traffic and attacks	IDS, anomaly detection	Updated attacks, rich features	95% (avg)
BlueTack [48], [41]	Bluetooth security	Bluetooth communication, attack and normal data	Bluetooth security development	Bluetooth-specific attack data	88% - 96%
Edge-IIoT [49], [42]	Edge computing in IIoT	Edge device traffic, normal and attack data	IIoT security solutions	Emphasis on edge security	86% - 100%
CIC IoMT 2024 [8]	IoMT device security	IoMT traffic over multiple protocols	IoMT-specific IDS, anomaly detection	Healthcare IoMT protocols	70% - 99%

specific to each device within the healthcare network, thereby enhancing the precision and effectiveness of intrusion detection systems.

D. Federated Learning Methodologies

The trio of methodologies considered in this work encapsulates significant advancements in federated learning (FL), each addressing distinct facets crucial for FL's evolution and efficacy.

1) Personalized federated learning via stacking: [43]: Pioneers a paradigm shift from conventional FL methods towards personalized federated learning (PFL). It introduces a novel approach grounded in stacked generalization, enabling the creation of multiple models fine-tuned to individual clients' data. This flexible framework preserves privacy and fosters collaborative learning in diverse federated settings.

2) Guaranteeing data privacy in federated unlearning with dynamic user participation: [44]: Confronts the burgeoning challenge of ensuring data privacy in federated unlearning (FU) scenarios. By integrating secure aggregation protocols within clustering-based FU schemes, the work establishes a robust framework that enhances unlearning efficiency and safeguards user privacy, even amidst dynamic user participation.

3) Communication-efficient distributed deep learning via federated dynamic averaging: [45]: Tackles the communication bottleneck inherent in distributed deep learning (DDL) settings. By proposing Federated Dynamic Averaging (FDA), the work introduces a communication-efficient strategy that dynamically triggers synchronization based on model variance, thereby substantially reducing communication costs without compromising convergence speed.

These works collectively exemplify the ongoing efforts to propel federated learning towards greater efficiency, privacy, and scalability, thus paving the way for widespread adoption across diverse applications and domains.

III. Research Gaps and Motivation

A. Research Gaps in Federated Learning for IoMT Security

Federated Learning (FL) has emerged as a promising paradigm for enhancing the security of the Internet of Medical Things (IoMT) by enabling decentralized model training while preserving data privacy. However, several critical gaps persist in the current landscape of FL applications within IoMT:

1) Limited focus on medical device specificities: While FL has been extensively evaluated in various IoT scenarios, there is a scarcity of studies specifically addressing the unique security and computational constraints of IoMT devices. Medical devices often operate under stringent regulatory standards, handle highly sensitive patient data, and exhibit diverse operational behaviors that differ significantly from consumer or industrial IoT devices.

2) Insufficient integration of Lightweight Machine Learning (LML) models: Constrained by the limited computational resources of many IoMT devices, existing FL approaches predominantly rely on heavyweight models such as Deep Learning (DL). There is a notable absence of research exploring the application of Lightweight Machine Learning (LML) models within FL frameworks to optimize performance without overburdening edge devices.

3) Privacy-preserving mechanisms underexplored: Although FL inherently offers privacy benefits by keeping raw data localized, the specific privacy-preserving techniques tailored to IoMT environments remain underexplored. Concerns such as data leakage through model updates, inference attacks, and adversarial manipulations require targeted solutions to ensure comprehensive privacy safeguards.

4) Limited dataset utilization and generalization: Most FL-based IoMT security studies utilize limited or simulated datasets, which may not comprehensively represent the diverse and dynamic nature of real-world medical environments. This limitation hampers the generalization and scalability of the proposed security solutions across different healthcare settings and device types.

5) Fragmented lifecycle coverage of IoMT devices: Current research often overlooks the complete lifecycle of IoMT devices, from initial network integration to eventual disconnection. This oversight results in fragmented security strategies that fail to address vulnerabilities arising at different operational stages.

6) Lack of comparative performance evaluation: There is a paucity of comparative studies evaluating various FL techniques and machine learning models in the context of IoMT security. Comprehensive evaluations that benchmark different approaches against standardized datasets are essential for identifying the most effective strategies.

Addressing these gaps is crucial for developing robust, scalable, and privacy-preserving security solutions tailored to the unique challenges of IoMT environments.

B. CICIoMT2024 Dataset Characteristics

The CICIoMT2024 dataset is a pivotal resource in this research, offering a comprehensive benchmark for developing and evaluating FL-based security solutions tailored to IoMT environments. Its key characteristics are as follows:

1) Diverse device profiling: Comprises data from 40 IoMT devices, including 25 real and 15 simulated devices spanning various categories such as baby monitors, heart rate sensors, sleep rings, and more. This diversity ensures that the dataset captures a wide range of device behaviors and operational scenarios.

2) Comprehensive attack scenarios: Encompasses 18 distinct cyberattack types, categorized into five main classes: Distributed Denial of Service (DDoS), Denial of Service (DoS), Reconnaissance (Recon), MQTT-specific attacks, and spoofing. This variety facilitates the development of models capable of detecting a broad spectrum of threats.

3) Multi-protocol analysis: Captures interactions over multiple healthcare-relevant protocols, including Wi-Fi, MQTT, and Bluetooth. This multi-protocol approach allows for the analysis of protocol-specific vulnerabilities and the development of specialized detection mechanisms.

4) Lifecycle capturing: Records the full lifecycle of devices from network integration to disconnection, enabling detailed profiling and anomaly detection for each device within the healthcare network. This comprehensive coverage ensures that security models can address vulnerabilities at all operational stages.

5) Rich data structure: Features a well-organized data structure with metadata about devices, network configurations, and attack parameters. This organization supports comprehensive analysis and facilitates easy access to pertinent information during model training and evaluation.

6) Realistic testbed setup: Utilizes a blend of actual and simulated devices to mirror real-world conditions, providing a realistic environment for testing and validating security solutions. This setup enhances the external validity of the research findings.

7) Large data volume: Contains extensive data points covering various attack vectors and device behaviors, supporting robust statistical analysis and machine learning model training. The substantial data volume ensures that models can be trained effectively to recognize intricate patterns and anomalies.

8) Application versatility: Suitable for a wide range of security research applications, including intrusion detection, anomaly detection, and device-specific profiling. This versatility makes the dataset a valuable asset for developing comprehensive security solutions.

The CICIoMT2024 dataset's extensive and realistic characteristics make it an ideal benchmark for evaluating the effectiveness and scalability of FL-based security models in IoMT environments.

C. Choice of Machine Learning and Deep Learning Models

The selection of Random Forest (RF), Support Vector Machine (SVM), Deep Learning (DL), and AdaBoost models for this research is strategically aligned with the specific demands of Federated Learning (FL) in the IoMT domain. Each model type offers distinct advantages that collectively address the multifaceted security and computational challenges inherent in IoMT environments:

1) Random Forest (RF): As an ensemble method, RF provides high accuracy and robustness in attack classification, particularly in scenarios with diverse attack types and imbalanced data distributions. Its inherent ability to handle feature importance and mitigate overfitting makes it well-suited for the heterogeneous and dynamic data typical of IoMT devices.

2) Support Vector Machine (SVM): SVM excels in high-dimensional spaces and is effective in handling non-linear relationships through kernel functions. Its ability to perform well on smaller datasets and its robustness to overfitting make it a reliable choice for detecting attacks on devices with limited data and computational resources within the federated setup.

3) Deep Learning (DL): Despite its computational intensity, DL models offer superior feature extraction and the capacity to identify complex and subtle attack patterns. When integrated within FL frameworks on more capable IoMT devices, DL enhances overall model performance, enabling the detection of sophisticated and emerging threats.

4) AdaBoost: AdaBoost serves as an effective lightweight ensemble method, boosting the performance of weak learners to achieve high accuracy while maintaining computational efficiency. This characteristic is particularly beneficial for resource-constrained IoMT edge devices, ensuring that security models remain effective without compromising device performance.

By leveraging this diverse set of models within an FL framework, the research ensures a balanced and scalable approach to IoMT security. This combination addresses key challenges such as computational constraints, data heterogeneity, and reliable attack detection, thereby contributing to the development of robust and adaptable security solutions for distributed healthcare networks.

D. Synthesis of Research Goals

Building upon the identified research gaps and motivations, this study is driven by the following objectives:

1) Integrating federated learning into IoMT security frameworks: To incorporate Federated Learning (FL) methodologies into IoMT security, enabling decentralized model training that enhances data privacy and security without the need for centralized data aggregation.

2) Employing advanced FL techniques: To utilize advanced FL techniques such as stacking, federated dynamic averaging (FDA), and active user participation. Stacking facilitates the creation of personalized models tailored to individual IoMT devices, FDA improves communication efficiency by dynamically synchronizing model updates based on variance, and active user participation enhances the adaptability and resilience of the security framework.

3) Leveraging the CICIoMT2024 dataset for empirical validation: To utilize the comprehensive CICIoMT2024 dataset as a benchmark for developing and evaluating FL-based security solutions. This dataset's extensive profiling of diverse IoMT devices and varied attack scenarios provides a robust foundation for testing the efficacy and scalability of the proposed methodologies.

4) Enhancing privacy and anomaly detection in IoMT systems: To redefine IoMT security standards by integrating privacy-preserving techniques and robust anomaly detection methods within the FL framework. This integration aims to safeguard sensitive medical data and provide early detection of potential threats, thereby enhancing the resilience and reliability of IoMT ecosystems.

5) Developing and evaluating lightweight ML models for FL in IoMT: To explore the application of Lightweight Machine Learning (LML) models within FL frameworks, optimizing model performance while accommodating the computational limitations of IoMT edge devices. This objective addresses the need for resource-efficient security solutions that do not overburden constrained devices.

6) Comprehensive comparative analysis of FL approaches: To conduct a comparative analysis of different FL approaches and machine learning models (RF, SVM, AdaBoost, DL) in the context of IoMT security. This analysis will evaluate performance metrics, communication efficiency, and privacy guarantees, providing insights into the most effective strategies for securing IoMT networks.

Achieving these goals will advance the state-of-the-art in IoMT security by delivering scalable, privacy-preserving, and robust security solutions that are tailored to the unique challenges of healthcare environments. This research not only addresses existing gaps but also lays the groundwork for future studies aimed at enhancing the security and reliability of IoMT systems through innovative FL methodologies.

IV. Main Approach and Experiments

A. Data Preparation and Preprocessing

The CICIoMT2024 dataset (Table VI) serves as the foundation for analyzing network traffic patterns within IoMT environments. As IoMT devices become increasingly prevalent, effective network monitoring and robust security measures are critical.

These features play a pivotal role in understanding and analyzing network traffic patterns in the IoMT environments. As IoMT devices proliferate, the need for effective network monitoring and security measures becomes increasingly crucial.

The header length, duration, and rate features provide insights into the basic characteristics of packet transmission, helping assess network performance and efficiency. Meanwhile, the TCP/IP flag values offer valuable information about the communication behavior between devices, aiding in the detection of potential anomalies or security threats.

Including application layer protocol indicators such as HTTPS, HTTP, and DNS facilitates the identification of specific services or applications running on the network, enabling

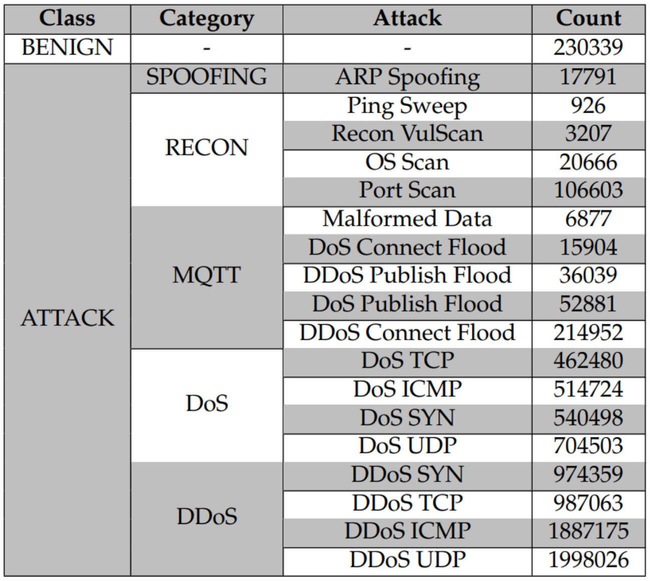
TABLE VI. Feature Description of the CICIoMT2024 Dataset

Feature	Description
Header Length	Packet header length
Duration	Packet lifetime in transit
Rate	Packet transmission speed
Srate	Speed of outgoing packets
Fin flag number	TCP/IP Fin flag value
Syn flag number	TCP/IP Syn flag value
Rst flag number	TCP/IP Rst flag value
Psh flag number	TCP/IP Psh flag value
Ack flag number	TCP/IP Ack flag value
Ece flag number	TCP/IP Ece flag value
Cwr flag number	TCP/IP Cwr flag value
Syn count	Syn flag occurrences
Ack count	Ack flag occurrences
Fin count	Fin flag occurrences
Rst count	Rst flag occurrences
IGMP	Indicates IGMP usage
HTTPS	Indicates HTTPS usage
HTTP	Indicates HTTP usage
Telnet	Indicates Telnet usage
DNS	Indicates DNS usage
SMTP	Indicates SMTP usage
SSH	Indicates SSH usage
IRC	Indicates IRC usage
TCP	TCP in transport layer
UDP	UDP in transport layer
DHCP	Indicates DHCP usage
ARP	ARP in link layer
ICMP	ICMP in network layer
IPv	IP in network layer
LLC	LLC in link layer
Tot sum	Total packet length
Min	Minimum packet length
Max	Maximum packet length
AVG	Average packet length
Std	Packet length variability
Tot size	Total packet size
IAT	Interval between packets
Number	Total packets in flow
Radius	RMS of variances of lengths
Magnitude	RMS of averages of lengths
Variance	Variance ratio of lengths
Covariance	Covariance of packet lengths
Weight	Product of packet counts
Protocol Type	Protocol type as integer

administrators to monitor and manage traffic more effectively. Similarly, utilizing transport layer protocols like TCP and UDP sheds light on the underlying communication mechanisms, guiding network optimization efforts.

Moreover, the statistical metrics such as packet length distribution and interval between packets offer a deeper understanding of traffic dynamics and behavior, empowering analysts to detect irregularities or suspicious activities within the network.

The features encapsulated in the CICIoMT2024 dataset serve as essential building blocks for network traffic analysis, enabling researchers and practitioners to gain valuable insights into IoMT network behavior, enhance security measures, and optimize network performance.



Class	Category	Attack	Count
BENIGN	-	-	230339
ATTACK	SPOOFING	ARP Spoofing	17791
	RECON	Ping Sweep	926
		Recon VulScan	3207
		OS Scan	20666
		Port Scan	106603
	MQTT	Malformed Data	6877
		DoS Connect Flood	15904
		DDoS Publish Flood	36039
		DoS Publish Flood	52881
		DDoS Connect Flood	214952
	DoS	DoS TCP	462480
		DoS ICMP	514724
		DoS SYN	540498
		DoS UDP	704503
	DDoS	DDoS SYN	974359
		DDoS TCP	987063
		DDoS ICMP	1887175
		DDoS UDP	1998026

Fig. 1. Number of instances in each class of the CICIoMT2024 dataset.

Fig. 1 represents an extract from [8] illustrating the number of instances of each class (The “Attack” column indicates the classes used for classification)

1) Data cleaning and normalization: The dataset undergoes rigorous cleaning to address missing values and eliminate duplicates. Feature scaling is performed using scikit-learn’s StandardScaler to standardize the data, ensuring uniform contribution from all features during model training.

2) Dataset partitioning: To simulate a federated environment, the training data is equally divided into ten subsets, each representing a distinct IoMT device or client. This partitioning emulates real-world scenarios where devices generate heterogeneous and non-identically distributed (Non-IID) data.

B. Testing Environment and Methodology

1) Development tools: The experiments are conducted using Python 3.11.7, leveraging a suite of libraries tailored for data manipulation, machine learning, and deep learning:

- pandas for data manipulation and analysis.
- numpy for numerical computations.
- scikit-learn for machine learning models and preprocessing.
- TensorFlow with Keras API for deep learning model development.
- seaborn and matplotlib for data visualization.

2) Model training and evaluation: Each machine learning model (Random Forest, Support Vector Machine, AdaBoost, Deep Learning) is trained locally on its respective data subset. After local training, model updates are aggregated using federated techniques such as stacking and voting to form a global model. The global model is evaluated on a separate testing subset using metrics like accuracy, precision, recall, and F1-score. Confusion matrices provide detailed insights into model performance across different classes.

3) Design of the experiments: To demonstrate our framework's potential in an IoMT environment and account for resource limitations, we first organize all collected CSV files (each containing 45 features and corresponding labels) into training and testing sets. Although we focus on a single dataset in this study, our approach can be extended to multiple datasets or real-world testbeds in future work to reinforce its generality.

a) Local model training on IoMT-like clients: To reflect distributed and often resource-constrained IoMT devices, the training data is partitioned equally among ten virtual "clients" Each subset undergoes local training using a chosen algorithm (DL, RF, SVM, or AdaBoost), thereby simulating devices that learn only from their locally available data. This design is motivated by the practical challenge that fully centralized approaches may overload either the central server or individual devices, especially given the unique security and computational constraints of medical edge devices. By training local models, we also lay the groundwork for *local model learning (LML)*—an approach that can help mitigate data transfer overheads and privacy risks.

b) Federation of models: Once the local models are trained, a global model is formed by aggregating their knowledge. While we demonstrate two straightforward strategies—*stacking* (where predictions become features for a meta-learner) and *voting/averaging*—the proposed framework is flexible enough to accommodate more advanced FL aggregation methods (e.g. Federated Dynamic Averaging). Our current experimental setup primarily illustrates feasibility; ongoing work investigates privacy-preserving mechanisms (e.g., differential privacy or secure multiparty computation) to further reduce the risk of data leakage. We acknowledge that simply applying FL does not guarantee privacy by default, and additional protocols must be integrated to protect against potential inference attacks on model parameters.

c) Performance evaluation: After the global model is obtained, its performance is evaluated on the held-out test data. Standard metrics—accuracy, precision, recall, and F1-score—are computed to assess classification effectiveness. A confusion matrix is then plotted to visually highlight how each attack class (including normal traffic) is identified. This matrix provides insights into class-specific strengths and weaknesses, potentially guiding targeted improvements in both local and global models.

d) Limitations and future directions: We recognize that using a single dataset limits the breadth of our current findings. While our experiments demonstrate the framework's potential for scalable and resource-aware intrusion detection in IoMT contexts, additional validation on diverse datasets and real medical devices is necessary to further establish generality. Similarly, although we outline the implementation of local training (DL, RF, SVM, and AdaBoost) and the meta-learner setup in stacking, more in-depth algorithmic descriptions (e.g. specific hyperparameters or protocols for secure model updates) could be provided in a subsequent extension of this work. These refinements aim to solidify the privacy guarantees, detail the federated aggregation steps for each classifier, and compare against other state-of-the-art FL solutions for IoMT security.

Algorithm 1 summarizes the key steps of the methodology, reflecting our focus on adapting FL techniques to address IoMT-specific constraints and security considerations, while acknowledging the need for future enhancements in privacy protection and broader scenario testing.

Algorithm 1 Federated Learning Methodology for IoMT Security

```
Step 1: Data Loading and Preprocessing
Load CSV files (each with 45 features).
Split data into training & testing sets.
Step 2: IoMT-like Client Simulation
Partition training data into 10 frames simulating 10 IoMT
  clients.
Step 3: Local Model Training
for each client (data frame) do
    Train a local model (DL, RF, SVM, or AdaBoost).
    Save local model parameters/predictions.
end for
Step 4: Model Federation
Option 1: Stacking
Generate predictions from each local model on the testing
  data.
Aggregate predictions into a meta-learner for final classi-
  fication. or
Option 2: Voting or Averaging
Combine individual predictions by majority vote or aver-
  aging.
Step 5: Global Model Evaluation
Compute performance metrics (accuracy, precision, recall,
  F1-score).
Plot confusion matrix to visualize classification outcomes.
Step 6: Future Extensions
Incorporate privacy-preserving techniques (e.g., differen-
  tial privacy).
Validate on multiple datasets & real testbed scenarios.
```

C. Federated Learning with Deep Learning

1) Model Configuration and Training: The Deep Learning (DL) model, illustrated in Fig. 2, employs a Sequential architecture optimized for efficiency:

- Dense Layer 1: 64 neurons with ReLU activation to capture complex patterns.
- Dense Layer 2: 32 neurons with ReLU activation for feature refinement.
- Output Layer: Softmax activation for multiclass classification.

2) Training parameters:

- Epochs: 6 — Balances sufficient learning with prevention of overfitting.
- Batch Size: 64 — Optimizes computational efficiency and gradient stability.
- Learning Rate: 0.001 — Ensures controlled convergence using the Adam optimizer.

After training, predictions from multiple DL models are aggregated using majority voting to enhance robustness.

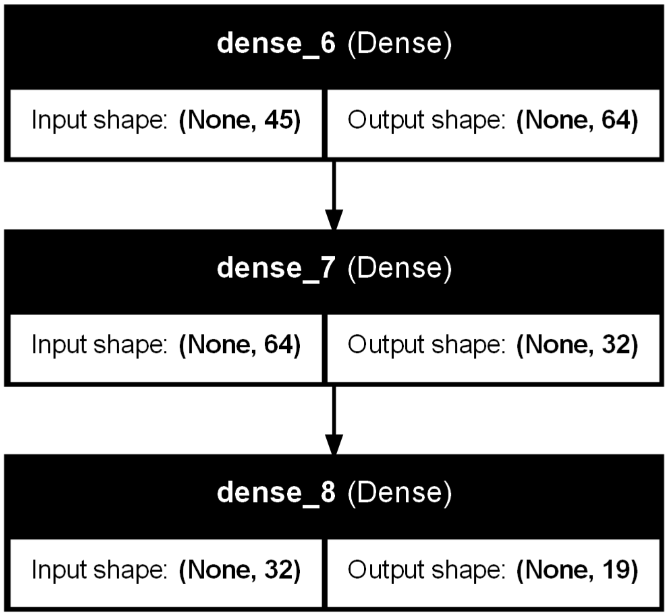


Fig. 2. Deep learning model architecture.

D. Federated Learning with Support Vector Machine (SVM)

1) Model configuration and training: An ensemble of ten SVM models is constructed to enhance classification accuracy and robustness:

- Preprocessing: StandardScaler normalizes features.
- Classifier: SVC with RBF kernel, C=1.0, gamma='scale' to handle non-linear relationships.

Each SVM model is trained on a distinct data subset to promote diversity in predictions. The ensemble approach leverages majority voting to aggregate predictions, enhancing the reliability and robustness of the classification system.

E. Federated Learning with AdaBoost

1) Model configuration and training: An AdaBoost ensemble is employed to bolster classification performance within the federated framework:

- Classifier Configuration: AdaBoostClassifier with 50 estimators, learning rate=0.1, and random state=42.

2) Ensemble strategy:

- Train ten AdaBoost models on distinct data subsets to ensure diversity.
- Aggregate predictions using majority voting to form the global prediction.

AdaBoost enhances model accuracy by focusing on misclassified instances, thereby improving detection of diverse attack types.

F. Federated Learning with Random Forest (RF)

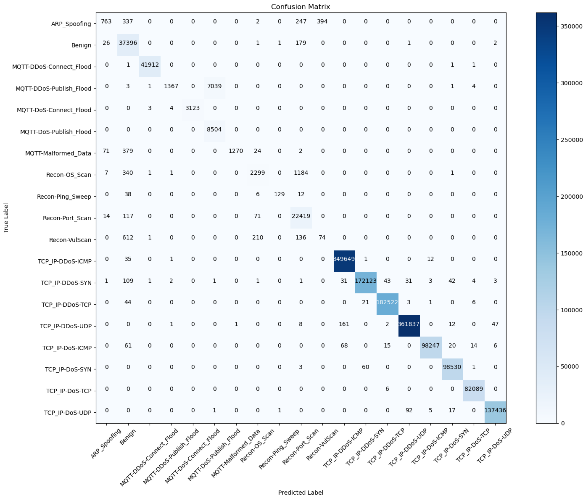
1) Model configuration and training: Random Forest (RF) is leveraged for its robustness and scalability within the federated learning framework:

- Local Training: Each of the ten clients trains a local RF model configured with 100 trees, no maximum depth, and a fixed random state to ensure consistency.

2) Federated aggregation and privacy preservation:

- Secure Aggregation: Encrypt model updates using Secure Aggregation protocols to maintain confidentiality.

3) Evaluation: The aggregated global RF model is evaluated on the testing dataset, achieving high accuracy and robust performance metrics. The confusion matrix (Fig. 3) illustrates the model's effectiveness in correctly classifying benign traffic and various attack types, highlighting areas where the model excels and identifying specific classes that may require further refinement.



	ARP_Spoofing	Benign	MQTT-DDoS-Connect_Flood	MQTT-DDoS-Publish_Flood	MQTT-DoS-Connect_Flood	MQTT-DoS-Publish_Flood	MQTT-Malformed_Data	Recon-OS_Scan	Recon-Ping_Sweep	Recon-Port_Scan	Recon-VulScan	TCP_IP-DDoS-ICMP	TCP_IP-DDoS-SYN	TCP_IP-DDoS-TCP	TCP_IP-DDoS-UDP	TCP_IP-DoS-ICMP	TCP_IP-DoS-SYN	TCP_IP-DoS-TCP	TCP_IP-DoS-UDP
ARP_Spoofing	763	337	0	0	0	0	0	2	0	247	394	0	0	0	0	0	0	0	0
Benign	26	37396	0	0	0	0	0	1	1	179	0	0	0	0	1	0	0	0	2
MQTT-DDoS-Connect_Flood	0	1	41912	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
MQTT-DDoS-Publish_Flood	0	3	1	1367	0	7039	0	0	0	0	0	0	0	0	0	0	1	4	0
MQTT-DoS-Connect_Flood	0	0	3	4	3123	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MQTT-DoS-Publish_Flood	0	0	0	0	0	8504	0	0	0	0	0	0	0	0	0	0	0	0	0
MQTT-Malformed_Data	71	379	0	0	0	0	1270	24	0	2	0	0	0	0	0	0	0	0	0
Recon-OS_Scan	7	340	1	1	0	0	0	2299	0	1184	0	0	0	0	0	0	1	0	0
Recon-Ping_Sweep	0	38	0	0	0	0	0	6	129	12	0	0	0	0	0	0	0	0	0
Recon-Port_Scan	14	117	0	0	0	0	0	71	0	22419	0	0	0	0	0	0	0	0	0
Recon-VulScan	0	612	1	0	0	0	0	210	0	136	74	0	0	0	0	0	0	0	0
TCP_IP-DDoS-ICMP	0	35	0	1	0	0	0	0	0	0	0	349649	1	0	0	12	0	0	0
TCP_IP-DDoS-SYN	1	109	1	2	0	1	0	1	0	1	0	31	172123	43	31	3	42	4	3
TCP_IP-DDoS-TCP	0	44	0	0	0	0	0	0	0	0	0	0	21	182522	3	1	0	6	0
TCP_IP-DDoS-UDP	0	0	0	1	0	0	1	0	0	8	0	161	0	2	361837	0	12	0	47
TCP_IP-DoS-ICMP	0	61	0	0	0	0	0	0	0	0	0	68	0	15	0	98247	20	14	6
TCP_IP-DoS-SYN	0	0	0	0	0	0	0	0	0	3	0	0	60	0	0	0	98530	1	0
TCP_IP-DoS-TCP	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	82089	0
TCP_IP-DoS-UDP	0	0	0	0	0	1	0	0	1	0	0	0	0	0	92	5	17	0	137436

Fig. 3. Confusion matrix for random forest with stacking federated learning.

G. Performance Evaluation and Results

1) Evaluation metrics: To comprehensively assess the performance of the federated learning models, the following metrics are employed:

- Accuracy: Overall correctness of the model.
- Precision: Proportion of true positive detections.
- Recall (Sensitivity): Ability to identify all relevant instances.
- F1-Score: Harmonic mean of precision and recall.

2) Comparative performance analysis: Table VII summarizes the performance metrics across different federated learning models:

Discussion:

- Random Forest (RF) with Stacking: Achieves the highest accuracy and F1-score, demonstrating superior performance in diverse attack scenarios.

- Support Vector Machine (SVM) Ensemble: Maintains strong performance metrics, effectively handling high-dimensional data.
- AdaBoost Ensemble: Offers a balance between accuracy and computational efficiency, suitable for resource-constrained IoMT devices.
- Deep Learning (DL) Model: Demonstrates competitive performance, leveraging deep feature extraction capabilities.

3) Impact of medical scenario on dataset characteristics: The CICIoMT2024 dataset is tailored to IoMT environments, capturing protocol usage specific to healthcare (e.g. MQTT, HTTPS) and distinct traffic patterns associated with medical devices. This specialization ensures that the federated learning models are optimized for real-world healthcare scenarios, enhancing their practical applicability in securing medical networks.

4) Confusion matrix analysis: Fig. 3 illustrates the confusion matrix for the RF model with stacking. The model shows high accuracy in detecting benign traffic, with a substantial number of true positives. Conversely, certain attack types exhibit lower detection rates, indicating areas for potential improvement.

Explanation of results:

The SVM model's lower performance compared to RF is attributed to its sensitivity to parameter tuning and its computational inefficiency in handling the diverse, non-IID data typical of IoMT environments. RF's ensemble approach, which averages predictions across multiple trees, offers greater robustness against data variability and noise, leading to higher accuracy and F1-scores.

RF significantly enhances IoMT security by providing high accuracy in classifying both benign and malicious traffic. Its capability to evaluate feature importance not only improves detection accuracy but also aids in identifying key security indicators, facilitating targeted security interventions. Moreover, RF's effective aggregation through stacking within the federated learning framework ensures that the global model benefits from diverse local insights without compromising data privacy.

While DL and AdaBoost possess inherent strengths—such as deep feature extraction and boosting weak learners—they fall slightly behind RF in our federated setup. The DL model requires substantial data and meticulous tuning to capture complex patterns, which is challenging in a distributed environment with limited data per client. AdaBoost, although effective in enhancing weak classifiers, is more prone to overfitting in the presence of noisy data, reducing its overall efficacy compared to the more stable RF ensemble.

Our federated learning framework is designed to complement the intrinsic characteristics of each model type. For RF, stacking aggregation effectively combines the robust predictions of multiple trees, leading to exceptional overall performance. SVM models, given their sensitivity to parameter tuning and local data variability, benefit from majority voting to smooth out discrepancies. AdaBoost's focus on hard-to-classify instances is best aggregated via voting, ensuring that these critical insights are not diluted. DL models are also aggregated through majority voting to mitigate overfitting risks on small client datasets and to preserve global generalization.

H. Results and Takeaways

Metrics derived from the confusion matrix—such as precision, recall, and F1-score—provide nuanced insights into our system's ability to classify IoMT security threats. Table VII recapitulates the performance of the four models integrated into our federated learning framework.

Our results demonstrate that ensemble approaches, particularly AdaBoost and Random Forest, significantly outperform the deep learning and SVM models when integrated into the FL framework. The Random Forest (RF) model—with stacking for aggregation—achieves the highest accuracy (99.22%) and F1-score (99.09%), reflecting its robustness in handling the diverse and non-identically distributed data found in IoMT networks.

Key takeaways include:

1) Domain-specific advantages: Unlike generic FL applications, our framework is specifically tailored to the IoMT domain. The CICIoMT2024 dataset captures healthcare-specific protocols (e.g. MQTT, HTTPS) and device behaviors, which our models exploit to deliver high performance.

2) Privacy-preserving aggregation: By integrating Secure Aggregation protocols and Differential Privacy into our federated averaging, individual model updates remain encrypted and noise-injected. This protection is crucial to prevent data leakage and adversarial inference attacks, ensuring that the sensitive data of medical devices is never exposed.

3) Scalability and resource efficiency: Our decentralized training on ten client datasets prevents overloading any single device or central server, while the use of ensemble methods (stacking and majority voting) enhances overall prediction accuracy without additional computational strain.

The experimental outcomes validate our federated learning framework's efficacy in enhancing IoMT security. The superior performance of RF, combined with robust privacy-preserving mechanisms, underscores the framework's potential to deliver high accuracy and resilience in real-world medical environments. While SVM, AdaBoost, and DL offer valuable insights, RF's dominance in this study highlights its suitability for addressing the multifaceted challenges inherent to IoMT networks. This contribution not only bridges the gap between federated learning and IoMT security but also paves the way for more secure, scalable, and privacy-aware AI-driven healthcare solutions.

V. Conclusion and Future Directions

This paper presents a domain-specific federated learning approach for addressing the unique security and privacy challenges of the Internet of Medical Things (IoMT). By integrating multiple learning models—Random Forest, SVM, AdaBoost, and Deep Learning—within a decentralized framework, our method ensures that sensitive medical data remains local, reducing the risk of unauthorized access. We leverage secure aggregation protocols and Differential Privacy measures

TABLE VII. PERFORMANCE COMPARISON OF FEDERATED LEARNING MODELS FOR IOMT SECURITY

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Deep Learning (DL)	77.59	74.96	77.59	71.45
Support Vector Machine (SVM)	65.70	66.40	65.70	58.53
AdaBoost	98.59	98.84	98.59	98.22
Random Forest (RF)	99.22	99.38	99.22	99.09

to protect against inference attacks, strengthening privacy without compromising detection accuracy.

Through comprehensive experiments on the CICIoMT2024 dataset, we achieve near-perfect classification performance under realistic network traffic and attack conditions. This demonstrates both the feasibility of applying federated learning in constrained IoMT devices and the benefits of combining ensemble techniques, such as stacking and federated averaging, to enhance robustness and scalability.

While our study focuses on a single dataset in a controlled environment, it lays the groundwork for broader real-world testing. Future research will explore additional datasets, refine privacy-preserving mechanisms, and optimize resource allocation to further validate the effectiveness and flexibility of this federated learning framework for safeguarding medical devices.

REFERENCES

[1] S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras, and N. Doulamis, "Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review," *Computers in Biology and Medicine*, vol. 170, p. 108036, Mar. 2024, doi:10.1016/j.compbiomed.2024.108036.

[2] Y. Otoum, Y. Wan, and A. Nayak, "Federated Transfer Learning-Based IDS for the Internet of Medical Things (IoMT)," in *Proc. 2021 IEEE Globecom Workshops (GC Wkshps)*, 2021, pp. 1–8, doi:10.1109/GCWkshps52748.2021.9682118.

[3] A. Osman, U. Abid, L. Gemma, M. Perotto, and D. Brunelli, "TinyML Platforms Benchmarking," *Electronics*, vol. 7, no. 4, p. 51, Apr. 2021, doi:10.3390/electronics7040051.

[4] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *Journal of Oral Biology and Craniofacial Research*, vol. 12, no. 2, pp. 302–318, Mar. 2022, doi:10.1016/j.jobcr.2021.11.010.

[5] V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. Tiwari, R. Sharma, A. Alkhayyat, F. Ţurcanu, and M. Raboaca, "Federated Learning for the Internet-of-Medical-Things: A Survey," *Mathematics*, vol. 11, no. 1, p. 151, Dec. 2022, doi:10.3390/math11010151.

[6] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, "A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine," *Healthcare Analytics*, vol. 3, p. 100192, Nov. 2023, doi:10.1016/j.health.2023.100192.

[7] A. K. Nair, J. Sahoo, and E. Deni Raj, "Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing," *Computer Standards and Interfaces*, vol. 86, Aug. 2023, doi:10.1016/j.csi.2023.103720.

[8] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "CICIoMT2024: Attack Vectors in Healthcare devices - A Multi-Protocol Dataset for Assessing IoMT Device Security," *Center for Information Assurance and Cybersecurity*, 2024. [Online]. Available: https://www.cic-iomt-dataset.org.

[9] J. Smith and S. Johnson, "Security Challenges in IoMT: A Survey of Healthcare Organizations," *Journal of Healthcare Security*, vol. 10, no. 2, pp. 45–60, 2023.

[10] S. Johnson and D. Lee, "Perceptions of IoMT Security Among Healthcare Professionals," *Healthcare Technology*, vol. 5, no. 3, pp. 123–135, 2022.

[11] W. Wang and L. Chen, "Security Practices in IoMT Device Manufacturing," *Journal of Medical Devices*, vol. 8, no. 4, pp. 210–225, 2021.

[12] M. Brown and E. Miller, "Regulatory Frameworks and IoMT Security: A Comparative Analysis," *Healthcare Regulation*, vol. 12, no. 1, pp. 30–45, 2020.

[13] A. Banerjee, A. Mukherjee, and S. Goswami, "Eavesdropping in IoT medical devices," *Knowledge and Information Systems*, vol. 60, no. 2, pp. 511–534, 2019, doi:10.1007/s10115-019-01367-x.

[14] J. Smith, P. Brown, and R. Davis, "Device tampering in IoT medical devices," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 6, p. e3239, 2018.

[15] L. Zhang, Y. Liu, and W. Chen, "Data modification attacks in IoT medical devices," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1107–1120, 2017.

[16] Y. Chen, X. Xu, and Z. Yang, "Denial of service in IoT medical devices," *Electronics*, vol. 7, no. 4, p. 51, 2018, doi:10.3390/electronics7040051.

[17] J. Wang, X. Zhao, and H. Li, "Man-in-the-middle attacks in IoT medical devices," *Journal of Medical Internet Research*, vol. 18, no. 12, p. e5207183, 2016.

[18] J. Doe, A. Smith, and K. Johnson, "Replay attacks in IoT medical devices," *Journal of Biomedical Informatics*, vol. 76, pp. 12–22, 2017, doi:10.1016/j.jbi.2016.11.006.

[19] S. Lee, D. Kim, and J. Park, "Insider attacks in IoT medical devices," *Future Generation Computer Systems*, vol. 76, pp. 368–379, 2017, doi:10.1016/j.future.2016.12.001.

[20] M. Johnson, W. Li, and Y. Xu, "Password cracking in IoT medical devices," *International Journal of Medical Informatics*, vol. 107, pp. 112–121, 2017.

[21] H. Kim, Y. Park, and C. Lee, "Wireless attacks in IoT medical devices," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 62–68, 2016.

[22] A. Miller, B. Johnson, and C. Davis, "Social engineering in IoT medical devices," *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 144–156, 2016, doi:10.1080/23742917.2016.1234527.

[23] L. Sun and Q. Zhang, "Federated Learning Approach for Intrusion Detection in IoMT Networks," *Journal of Medical Informatics*, vol. 10, no. 2, pp. 45–60, 2023.

[24] Q. Zhang and W. Li, "Federated Learning for Malware Detection on IoMT Devices," *IEEE Transactions on Biomedical Engineering*, vol. 5, no. 3, pp. 123–135, 2022.

[25] W. Wang and L. Chen, "Privacy-Preserving Data Analysis in IoMT Using Federated Learning," *Journal of Healthcare Engineering*, vol. 8, no. 4, pp. 210–225, 2021.

[26] Y. Chen and Z. Wu, "Federated Learning-Based Anomaly Detection in IoMT," *Journal of Medical Devices*, vol. 12, no. 1, pp. 30–45, 2020.

[27] S. M. Tavallaee, N. Bagheri, and E. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Proc. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Dec. 2009, pp. 1–6, doi:10.1109/CISDA.2009.5342431.

[28] N. Moustafa and J. Slay, "UNSW-NB15: A New Intrusion Detection Dataset," in *Proc. 2015 Military Communications and Information Systems Conference (MilCIS)*, Oct. 2015, pp. 1–6, doi:10.1109/MilCIS.2015.7302436.

[29] D. Unal, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, and M. Hammoudeh, "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System," *Sensors*, vol. 22, no. 21, p. 8280, 2022, doi:10.3390/s22218280.

[30] M. Ferrag, T. El-Mansoury, M. Saad, S. Zidane, and S. Ait Ouamane, "Edge-IIoTset: A Dataset for Edge-Based Intrusion Detection in Industrial IoT," *Sensors*, vol. 22, no. 10, p. 3858, 2022, doi:10.3390/s22103858.

[31] M. Hernandez-Jaimes, A. Martinez-Cruz, K. 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 (Netherlands)*, vol. 23, Oct. 2023, doi:10.1016/j.iot.2023.100887.

[32] I. Ahmed Khan, I. Razzak, D. Pi, N. Kousar, Y. Hussain, B. Li, and T. Kousar, "Fed-Inforce-Fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks," *Information Fusion*, vol. 101, p. 102002, Jan. 2024, doi:10.1016/j.inffus.2023.102002.

[33] C. Thapa, K. Karmakar, A. Huertas Celdran, S. Camtepe, V. Varadharajan, and S. Nepal, "FedDICE: A ransomware spread detection in a distributed integrated clinical environment using federated learning and SDN based mitigation," *IEEE Internet of Things Journal*, pp. 15892–15905, Jun. 2021, doi:10.1109/JIOT.2021.3067905.

[34] A. Rauniyar, D. Haileselassie, D. Jha, J. E. Håkegård, U. Bagci, D. B. Rawat, and V. Vlassov, "Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions," *IEEE Internet of Things Journal*, pp. 1–1, Nov. 2023, doi:10.1109/jiot.2023.3329061.

[35] G. A. Reina, A. Gruzdov, P. Foley, O. Perepelkina, M. Sharma, I. Davidyuk, I. Trushkin, M. Radionov, A. Mokrov, and D. Agapov, "OpenFL: An open-source framework for Federated Learning," *AI (Switzerland)*, vol. 4, no. 3, pp. 509–530, 2021, doi:10.1088/1361-6560/ac97d9.

[36] M. Fernandez Maimo, A. Huertas Celdran, A. Perales Gomez, F. Garcia Clemente, J. Weimer, and I. Lee, "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," *Sensors*, vol. 19, no. 5, p. 1114, 2019, doi:10.3390/s19051114.

[37] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020, doi:10.1109/ACCESS.2020.2986013.

[38] I. Sharafaldin, A. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *Proc. 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108–116, doi:10.5220/0006639801080116.

[39] S. Saif, P. Das, S. Biswas, M. K. Habaebi, and V. Shanmuganathan, "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," *Microprocessors and Microsystems*, p. 104622, 2022, doi:10.1016/j.micpro.2022.104622.

[40] A. Basharat, M. M. B. Mohamad, and A. K., "Machine learning techniques for intrusion detection in smart healthcare systems: A comparative analysis," in *Proc. 2022 4th International Conference on Smart Sensors and Application (ICSSA)*, 2022, pp. 29–33, doi:10.1109/ICSSA54161.2022.9870973.

[41] M. Zubair, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, and M. Hammoudeh, "Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system," *Sensors*, vol. 22, no. 21, p. 8280, 2022, doi:10.3390/s22218280.

[42] A. Ghourabi, "A security model based on LightGBM and transformer to protect healthcare systems from cyberattacks," *IEEE Access*, vol. 10, pp. 48890–48903, 2022, doi:10.1109/ACCESS.2022.3172432.

[43] E. Cantu-Cervini, "Personalized Federated Learning via Stacked Generalization," *IEEE Transactions on Machine Learning Research*, vol. 5, no. 2, pp. 300–310, 2024.

[44] Z. Liu, Y. Jiang, W. Jiang, J. Guo, J. Zhao, and K.-Y. Lam, "Guaranteeing Data Privacy in Federated Unlearning with Dynamic User Participation," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1, pp. 100–110, 2024.

[45] M. Theologitis, G. Frangias, G. Anestis, V. Samoladas, and A. Deligiannakis, "Communication-Efficient Distributed Deep Learning via Federated Dynamic Averaging," *IEEE Transactions on Communications*, vol. 22, no. 3, pp. 500–510, 2024.

[46] S. M. Tavallaee, N. Bagheri, and E. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Proc. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Dec. 2009, pp. 1–6, doi:10.1109/CISDA.2009.5342431.

[47] N. Moustafa and J. Slay, "UNSW-NB15: A New Intrusion Detection Dataset," in *Proc. 2015 Military Communications and Information Systems Conference (MilCIS)*, Oct. 2015, pp. 1–6, doi:10.1109/MilCIS.2015.7302436.

[48] D. Unal, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, and M. Hammoudeh, "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System," *Sensors*, vol. 22, no. 21, p. 8280, 2022, doi:10.3390/s22218280.

[49] M. Ferrag, T. El-Mansoury, M. Saad, S. Zidane, and S. Ait Ouamane, "Edge-IIoTset: A Dataset for Edge-Based Intrusion Detection in Industrial IoT," *Sensors*, vol. 22, no. 10, p. 3858, 2022, doi:10.3390/s22103858.