Received: November 12, 2023. Revised: January 25, 2024. 412

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Federated Learning-based Routing Vulnerability Analysis and Attack Detection for Healthcare 4.0

K. Kowsalyadevi[1]* N. V. Balaji[1]

[1]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India*
* Corresponding author's Email: [1]kowsalyamphilcs@gmail.com

Abstract: Industrial 4.0 technological breakthroughs highly impact healthcare 4.0 and enable transformative impact on the healthcare system by shifting towards efficient, patient-centric, data-driven, and robust global healthcare services. This paper presents a robust security framework; federated learning (FL) based RPL vulnerability analysis and attack detection (FRVA), for ensuring secure Healthcare 4.0. The FRVA is proposed to defend the RPL-healthcare 4.0 against multiple attacks by applying deep learning-based fuzzing and FL-enabled hybrid learning. RPL vulnerabilities are analyzed using randomly generated inputs by deep learning-based fuzzing. Further, it feeds the RPL vulnerability-rich fuzzed output dataset to the FL-hybrid learning model. The second model improved the customized local learning models using globally shared information according to FL, resulting in high learning accuracy with precise attack detection. The proposed FRVA runs the vulnerability analysis and attack detection at the edges to prolong the network lifetime with high security. Moreover, the performance of the FRVA is validated through Python-based simulations using different metrics. The simulation results demonstrate that the proposed FL-based hybrid CNN-LSTM strategy enhances the accuracy by 5.55% and 12.9%, respectively, compared with the individual CNN and LSTM methods. It also enhances the accuracy by 25.83% and 5.97% than the other conventional FL-based detection strategies.

Keywords: Healthcare 4.0, RPL security, Vulnerability analysis, Dataset construction, Cooja simulator, Deep learning-based fuzzing, Federated learning (FL), Attack detection.

1. Introduction

The global economy is transitioning to Industry 4.0, symbolizing the move towards digitalization and automated environments connected with cyber-physical systems. By utilizing the technological advancements in information and communication technologies, Healthcare 4.0 creates a significant shift towards enhanced healthcare delivery, enables global collaboration, improves patient outcomes, and enables potential innovations in healthcare by opening avenues for continual adaptation of advancements in future technology. Medical 4.0 envisions a highly linked healthcare system that provides more efficient and timely medication services to patients by making healthcare services available anytime to everyone. The Internet of Things (IoT) is important in connecting smart healthcare devices anytime and anywhere through any network [1]. It allows a patient to be connected to the wireless network and collect sensitive patient data through IoT. The advancement of Medical 4.0 technology allows healthcare providers to make better and more informed decisions [2]. Thus, it saves time, improves accuracy, and increases efficiency by creatively employing the latest information and communication technologies. Routing protocol for low-power and lossy networks (RPL) is a distant vector protocol supporting the 6LoWPAN adaptation layer for wireless sensor networks and resource-constrained devices by proficiently managing the limited power, memory, and processing capacities. This protocol yields substantial benefits in the healthcare domain that enable patient care, operational efficiency, and data-driven decision-making processes by establishing dependable and efficient communication routes among IoT devices. However, security is the major

concern in such types of protocols. The interconnectivity of IoT devices creates a vulnerability that can be exploited by malicious entities, leading to man-in-the-middle attacks where attackers can manipulate and intercept critical patient data during transmission. Within the IoT environment, the RPL protocol is vulnerable to various kinds of internal and external attacks [3]. Apart from that, some novel attacks highly impact the security of healthcare 4.0 and lead to life-threatening impacts on patient care.

Implementing robust defenses against this spectrum of attacks is crucial to guaranteeing accessibility, privacy, and security of healthcare services and patient data [4]. Conventional security solutions based on cryptography are not well-suited for ensuring the security of RPL-based networks owing to poor security keys and heavyweight operations [5]. The rise of resource-constrained devices and their integration with the internet has brought about significant cybersecurity vulnerabilities. These vulnerabilities pose threats to the security of users, potentially exposing them to various malicious threats [6]. A finite state machine (FSM) vulnerability was discovered that effectively identifies security vulnerabilities like sinkholes, selective-forwarding, and hello flood attacks in RPL [7]. RPL contains many exploitable vulnerabilities when an unauthorized node joins the IoT-low power lossy network, allowing attackers to launch insider attacks that drain or deplete resources from the network and decrease performance [8]. Federated learning (FL) plays a crucial role in medical healthcare due to its unique attributes aligning with the sector-specific demands for providing distributed intelligence for IoT devices capable of detecting a broad spectrum of attacks and assisting with network defense solutions. Improving the accuracy and reliability of ML models used in medical applications is essential. By combining data from numerous sources, models can be trained on multiple representative and diverse datasets for improving disease prediction, diagnostic accuracy, and treatment recommendation. FL has become a potential solution, offering globally shared knowledge from disparate healthcare sources while upholding patient data and privacy processing. FL addresses some demand by spreading machine and deep learning models to local devices, using the computing power of all clients, like routers, to develop a powerful attack defense mechanism with a higher detection rate [9, 10]. This paper aims to propose federated learning (FL) based RPL vulnerability analysis and attack detection (FRVA), a novel vulnerability analysis and attack detection method for RPL-healthcare 4.0 by utilizing deep learning fuzzing and new-generation FL algorithms.

1.1 Contributions

The main contributions of the proposed work are as follows.

- The primary objective of this work is to enhance the security and efficiency of RPL-based communication in Healthcare 4.0 by integrating deep learning-fuzzing-based vulnerability analysis and new-generation FL-based vulnerability detection.
- Firstly, the deep learning-fuzzing model integrates the RNN algorithm to analyze the vulnerabilities in the collected raw dataset. It generates different random attack patterns by determining wider RPL-Healthcare 4.0 vulnerabilities.
- Secondly, the proposed work applies a new generation FL model over the generated dataset and neglects the current data updating issues through incremental learning in which the recent attack data is partially updated to the established dataset. Thus, it enhances vulnerability detection accuracy in a distributed hospital 4.0 environment.
- The vulnerability detection integrates the combination of CNN-LSTM for vulnerability detection at the edges, resulting in efficient resource management and various attack detection. The globally shared model-based relearning of CNN-LSTM also improves learning accuracy.
- Finally, the efficacy of the vulnerability and attack model is analyzed using the Contiki/Cooja simulator. The proposed work utilizes various metrics with different nodes and attacker scenarios for analysis.

1.2 Paper organization

The remaining part of the paper is organized as follows. Section 2 briefly surveys the works related to RPL vulnerability analysis and detection to analyze the gaps. Further, section 3 describes the problem statement, system architecture, and attack model. Section 4 provides an overview of the proposed work with two methods: vulnerability analysis and attack detection. Consequently, section 5 shows the performance settings and results obtained using various metrics and scenarios. Finally, section 6 concludes this paper.

2. Literature survey

Attack detection enhances cybersecurity by identifying and mitigating threats from interconnected devices and is crucial in improving the integrity and operational continuity of IoT ecosystems. This section surveys the latest research on machine learning, deep learning, and FL techniques for attack detection in RPL using IoT networks.

2.1 Vulnerability analysis in RPL-based approaches

A vulnerability discovery method based on finite state machines (FSM) is presented to assess the security vulnerabilities within RPL [7]. This approach effectively identifies sinkhole attacks, selective-forwarding attacks, and hello flood attacks. In work [11], Industrial Internet of Things (IIoT) protocols and associated vulnerabilities are presented. It conducts an IIoT system vulnerability assessment and discusses using ML to combat susceptibility. Also, the literature studies on effective ML-based IDS for SCADA systems are reviewed. In paper [12], an ensemble learning-based IDS (E-ADS) using a fog cloud architecture was presented in an IoMT environment. To tackle heterogeneous and dynamic networks, a framework for implementing secure systems has been proposed as Software as a Service (SaaS) on the fog side and Infrastructure as a Service (IaaS) on the cloud side. However, feature selection techniques need to be considered to optimize and design a prototype of this model to verify its performance in a real-time fog cloud scenario. In paper [13], the research focuses on assessing the vulnerability of an objective function (OF) within the RPL protocol, which involves investigating rank attack manipulation and two widely used OFs, namely objective function zero (OF0) and minimum rank with hysteresis objective function (MRHOH). An analysis of energy consumption and packet delivery ratio is done in both malicious and non-malicious scenarios. The conventional vulnerability analysis strategies incur high false positives due to the utilization of a single strategy for analysis. Hence, designing hybrid algorithms to improve vulnerability analysis accuracy jointly is crucial.

The article [14] presents some observations that could serve as a basis for developing methods to prevent the misuse of rank property vulnerabilities. A solution to a significant security weakness in RPL fabricated parent change is introduced through an effective intrusion detection system (IDS) [15]. The parental change control RPL (PCC-RPL) mitigates unauthorized parent changes by implementing a trust-based mechanism. In PCC-RPL, each parent consistently monitors the behavior of its child nodes. Any malicious activity detected by a parent reduces the trust level associated with the child and alerts the root node by transmitting a suspicious message. The article [16] addresses the security of IoT networks by exploiting vulnerabilities in the message queuing telemetry transport (MQTT) protocol. To discover new security vulnerabilities in MQTT, a fuzzy attack approach was proposed to detect security breaches. Using a fuzzing approach on Docker at a modest scale is effective in detecting a variety of MQTT security issues. However, a plan is required to improve the automatic generation of additional dangerous situations. A fuzzing test approach [17] was proposed and implemented in a heterogeneous environment. A fuzzing framework is developed to identify new program regions in a black box-based input, output, and delta time test. However, a hypothesis-test-based method is needed to reduce the testing time. Albeit, the existing fuzzing-based vulnerability analysis models lack the ability to determine novel attacks with wider knowledge. Thus, it diminishes the vulnerability distribution data in fuzzy outputs, a major concern in I4.0 applications.

2.2 Federated learning-based IoT attack detection approaches

In [18], an optimized FL model called optimized FL-securing RPL (OFL-SRPL) was introduced to enhance the security of RPL in advanced metering infrastructure (AMI) devices. OFL-SRPL employs an ensemble of classifiers sequentially, each with its unique loss function, to improve the final decision quality while reducing the communication overhead of FL. An FL framework [19] was utilized to enhance learning estimation in IoT networks. An optimization problem was formulated to generate RL-based Q-values for DODAG construction. The federated routing learning (FRL) paradigm was introduced to avoid overestimating collision information. A federated transfer-learning-assisted customized distributed IDS (FT-CID) was proposed in [20] to detect RPL intrusions within heterogeneous IoT environments. The FT-CID design process is decomposed into three steps: dataset collection and preprocessing, FTL-assisted edge-enabled IDS learning, and final intrusion detection. In [21], a federated learning architecture was introduced to detect intruders. Similarly, FL-based learning for detecting zero-day botnet attacks [21] was proposed to enhance the data privacy

concept in IoT edge devices. It did not investigate advanced FL algorithms' potential to enhance attack detection. The existing works utilize a centralized single machine learning strategy for training, which often fails to create consistent global knowledge due to a lack of multiple algorithm-based decision-making.

Consequently, as exemplified by HT-Fed-GAN [28], a federated generative model employs a novel model called federated variational Bayesian Gaussian mixture to tackle the challenge of multimodal distributions. It introduces privacy-preserving decentralized data modeling by utilizing the federated conditional GAN. For proactive intrusion recognition within IoT networks using decentralized on-device data, an FL-based anomaly detection approach [29] has been proposed. The smart healthcare framework in [30], named FRESH, shares physiological data collected from wearable devices by applying FL and ring signature defense from the attacks. Edge computing devices process these data. This architecture in [31] formulates the data sharing challenge as a machine learning problem while integrating privacy-preserving FL. However, the decentralized nature of FL poses novel security challenges that are not effectively addressed in the existing works. Therefore, careful design of FL approaches with precise vulnerability analysis strategies is essential to improve the performance of healthcare I4.0.

2.3 Research gaps

There are two main gaps in the survey. Firstly, most existing fuzzing methods exploit general fuzzer and boxing fuzzing methods for vulnerability analysis. Since the general fuzzer and other fuzzing techniques incur high manual analysis and minimize the distributions of vulnerability data in fuzzy outputs, thus, it leads to creating many errors owing to misunderstandings of protocol specifications. Learning-based fuzzing methods can improve the vulnerability data distributions in its output with high automation. Secondly, despite advances in deep learning algorithms for RPL attack detection and identification of evolving attackers, crafting an effective FL model for medical devices requires careful consideration. FL performance balances accuracy and communication rounds, with excessive message transmission causing data loss and decision inaccuracies. Using a single classifier for training often falls short of creating a harmonized global learning model that ensures consistent knowledge. Most FL schemes adopt the FedAvg approach, increasing communication rounds and inefficiently allocating computation resources regardless of client data accuracy. It can lead to prolonged FL training sessions with minimal accuracy gains. Additionally, the weighted average favours clients with larger local training sets, potentially missing short attacks with out-of-distribution features. Moreover, the existing works jointly consider the vulnerability analysis and FL attack detection strategies, resulting in poor detection performances due to a lack of wider attack knowledge distribution. Also, they increase the error due to the ineffective vulnerability knowledge. To ensure secure communication in Healthcare 4.0, there is a critical need for combined vulnerability analysis and attack detection in RPL routing. Therefore, the proposed model integrates vulnerability analysis and an FL-based attack detection model to accomplish seamless I4.0 performance with high security.

3. Preliminaries

This section defines the preliminary information like the RPL introduction, system model and threat model related to the proposed model.

3.1 An introduction to RPL

The proactive RPL routing protocol is mainly designed for resource-constrained, low-power, and lossy IoT environments. The RPL protocol design primarily supports devices with limited processing capabilities and the network environment characterized by unreliable links, high packet loss, and low bandwidth. The RPL routing proactively builds and maintains DODAGs to ensure a loop-free routing path based on the specific objectives to fulfill the IoT needs. RPL utilizes the DODAG structure to organize from the single root node to multiple leaf nodes. The rank metric used to represent the position of nodes, nodes close to the root node have a lower rank. The objective Function (OF) guides the nodes to make routing decisions, potential parent selection and rank calculation. The destination advertisement and route discovery take place by using control messages. The control packet types are described in Table 1.

RPL routing supports multiple instances on the network with different objective functions to flexibly support diverse application requirements. The local repair mechanism detects a problem with a link and initiates a local repair operation without altering the existing DODAG structure.

3.2 Problem formulation

Vulnerability analysis is considered a

Table 1. Control packet types of RPL

Name	Direction of flow	Description
DODAG Information Solicitation (DIS)	Node to Root node	Connection request
DODAG Information Object (DIO)	Root node to Nodes	Advertise information about DODAG
Destination Advertisement Object (DAO)	Node to parent node	Child node Request
Destination Advertisement Acknowledgment (DAO-ACK)	Parent node to node	The child node requests acknowledgment
Control Information (CON)	Parent node to node	Control message

classification problem. The primary aim is to design a fuzzer to classify the data using the information learned from labeled datasets. The process involved is described as follows: Let n be the number of hospitals, and the medical data be defined as (dj, yj) where $d_j \in D$ and $l_j \in L$, where D represents the set of medical data/patient information and $L = \{0,1\}^j$ represents the label of the patient information, 0 for legitimate and 1 for vulnerable, and j represents the number of instances in datasets. Each domain collects the information from its environment and forms a private dataset D_n. Further, it exploits D_n to train a local L model at each aggregation round *k*. Local models are updated for σ FL local updates. For each *k*, the Federated aggregator (FA) randomly selects a subset of the local model S^n and aggregates all the parameters from S^n to generate an updated global model G_t, where t is the present aggregation round. The aggregation server sends G_t to all local models, and the local models update the G_t with their local dataset at $k + 1$. The problem of RPL attack detection in federated environments can be formulated as the maximization of detection accuracy (DA) of G_t on unbalanced, non-independent and identically distributed data across hospitals while minimizing total FL time. The objective function Θ is described as follows.

$$\Theta = \mathrm{DA} - \alpha * \mathrm{Error}$$

3.3 System model

Various IoT medical devices, like wearable sensors, generate medical data. Electronic health record (EHR) systems, health information exchange (HIE) platforms, and hospital networks provide access to patient data and network traffic. These local data from N hospitals are sent to the nearby base station using RPL routing. In the network layer, many routing attacks may affect the data. The architecture of the proposed model is shown in Fig. 1. When the local data from different sources reach the edge layer, two operations are performed on the edge: vulnerability analysis and attack detection. An analyzer is employed to keep track of their network data for vulnerability analysis and to check whether the local data has any vulnerability. Once the vulnerability analysis is completed, the dataset is created for training the local models collaboratively without sharing sensitive data. A central server coordinates the federated learning process.

Each medical device or data source is a local client with its own dataset. Local clients train their models on their respective datasets in the edge layer while keeping the data decentralized and secure. The FL server periodically aggregates model updates to create a global model. To integrate the models and develop a better attack detection system with optimum parameters, the federated aggregator is used in a cloud server to aggregate and combine model updates from multiple participating clients to create a global model without centralizing the raw data. It ensures that learning across decentralized devices occurs effectively while preserving data privacy. When vulnerabilities or attacks are detected, the system can take various actions, including generating alerts and notifications, isolating compromised devices or network segments, and logging and reporting incidents for further investigation.

3.4 Threat model

Various security concerns exist in RPL routing, including the potential for malicious nodes to execute disruptive actions. Additionally, there is the risk of spoofing attacks, wherein nodes impersonate legitimate devices or routers to manipulate routing decisions. Therefore, safeguarding RPL routing involves mitigating these risks to ensure dependable, efficient, and secure routing in IoT environments. The proposed work aims to detect eight types of vulnerabilities like rank, version number, OF, Sybil, worst parent, DoS, zero-day, and novel attacks over RPL-enabled healthcare 4.0.

Rank: The malicious device aims to increase or decrease the rank value, intending to disrupt the RPL routing functions.

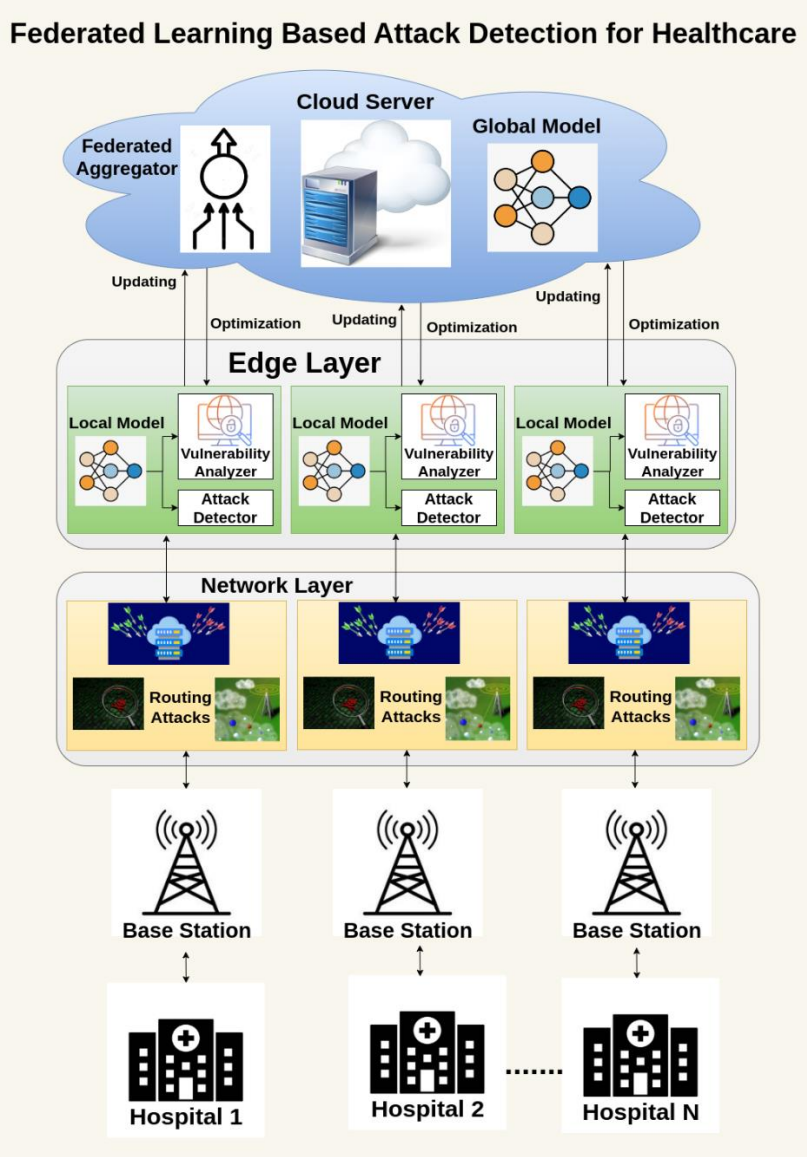


Figure. 1 FL-based attack detection for healthcare

Version number: It is highly related to DoS, which is inaugurated by escalating the RPL control traffic during the global repair mechanism.

OF: The malicious nodes target to launch various types of attacks like rank and parent by disrupting the normal OF-based DODAG construction process.

Sybil: In this type, the malicious node spoofs different real identities of various devices to inject malicious healthcare data into the network.

Worst parent: The malicious node aims to select sub-optimal RPL paths for data transmission, and thus, it creates improper network resource utilization.

DoS: The malicious device denies the network services to the legitimate devices by supporting the attacking behaviors.

Zero-day: It is unknown to the RPL security mechanisms, and it happens first time in the network.

Novel: It does not match the well-known vulnerabilities and is very different in the network system.

4. Design overview of proposed model

The main intention of the proposed work is to improve vulnerability detection accuracy with eight numbers of attacks through effective vulnerability analysis and FL deep learning models. The proposed work design is explained using two steps: RNN-fuzzing-based vulnerability analysis and NGFL-based vulnerability detection. Firstly, the RNN-fuzzing in edge healthcare 4.0 devices analyses different vulnerabilities with a deep learning strategy. Further, it generates a sub-dataset at each device to construct a novel RPL-Healthcare 4.0 dataset. Secondly, the NGFL model utilizes the

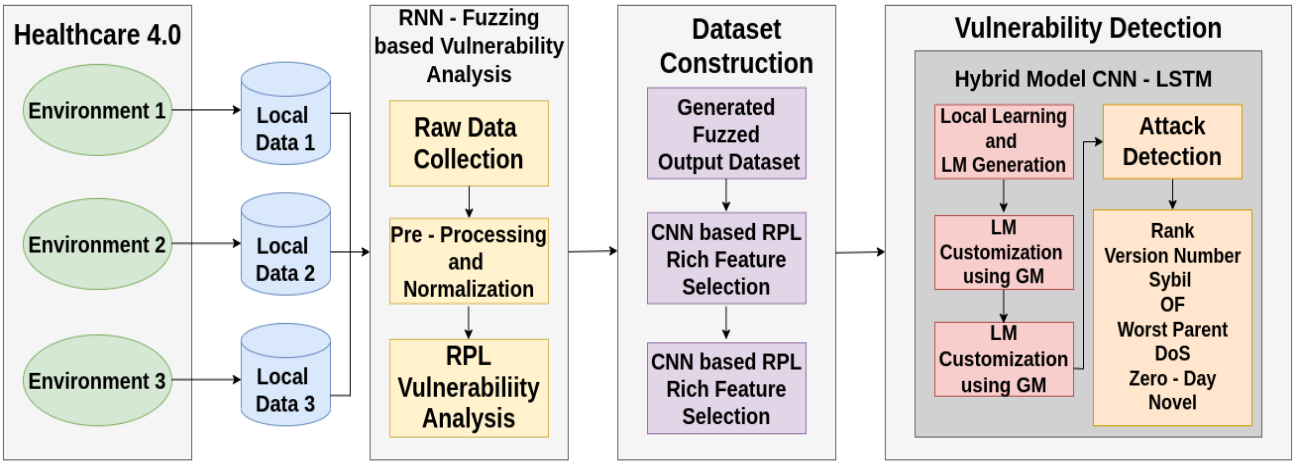


Figure. 2 Design overview of proposed methodology

advantages of CNN-LSTM to generate the local models at the edges. The generated local models are shared with the cloud server for generating a global model using a contextual weighted aggregation model. By combining the various local models of different edges in a distributive manner, the proposed work optimizes the learning accuracy of customized CNN-LSTM of edges and maximizes vulnerability detection accuracy. Moreover, the proposed work improves the multiple vulnerability detection accuracy by integrating a fuzzing vulnerability analysis and FL deep learning-based detection model, as shown in Fig. 2. By executing the proposed algorithms at edges, this work effectively manages the resource consumption efficiency and improves the lifetime of healthcare 4.0.

4.1 RNN-fuzzing-based vulnerability analysis

With the resource limitation nature of healthcare 4.0 devices and the minimum fundamental security nature of RPL routing protocol, RPL-healthcare 4.0 is vulnerable to different attacks. To enhance the attack detection accuracy and minimize the computation burden associated with large datasets, analyzing such vulnerabilities is crucial before straightly inputting the collected healthcare 4.0 data into attack detection. Fuzzing is a suitable method that produces random inputs to determine the vulnerabilities or unexpected behavior through better analysis of the raw input data Healthcare 4.0. Therefore, the proposed FRVA utilizes the recurrent neural network fuzzing model based fuzzing to analyze the various types of RPL vulnerabilities and to generate a vulnerability-rich fuzzing dataset for attack detection. The deep learning-based fuzzing model can analyze or detect the network vulnerabilities in the healthcare 4.0 scenario with minimum cost and computations. Therefore, the proposed FRVA integrates the RNN-fuzzing method to generate the RPL vulnerability-rich data for deep learning-based attack detection.

4.1.1. Raw dataset construction

Generally, the benchmark IoT datasets comprise well-known vulnerabilities like Rank, Version number, OF, Sybil, and worst parent. However, they are outdated and lack recent normal and attack traffic related to Healthcare 4.0. Hence, zero-day and novel vulnerabilities are created by considering the current network traffic to evaluate Healthcare 4.0 precisely. Zero-day and novel attacks have a high impact on the performance of healthcare 4.0, and it is very difficult to detect such attacks. Thus, the proposed work intends to construct the RPL-healthcare 4.0 dataset with normal and vulnerability information Rank, Version number, Worst parent, Sybil, DoS zero-day, and novel. The proposed model constructs the dataset by running the Contiki NG, shown in Fig. 3.

4.1.2. RNN-fuzzing method

The RNN-fuzzing is a deep neural network fuzzing model that exploits multiple layers of deep learning strategy to generate the output fuzzing RPL-healthcare 4.0 data. The RNN strategy for fuzzing bypasses the constructing protocol specification process of fuzzing by improving the automata level, and thus, it reduces the workload. It does not produce logic errors or human negligence, which are majorly caused by protocol specification

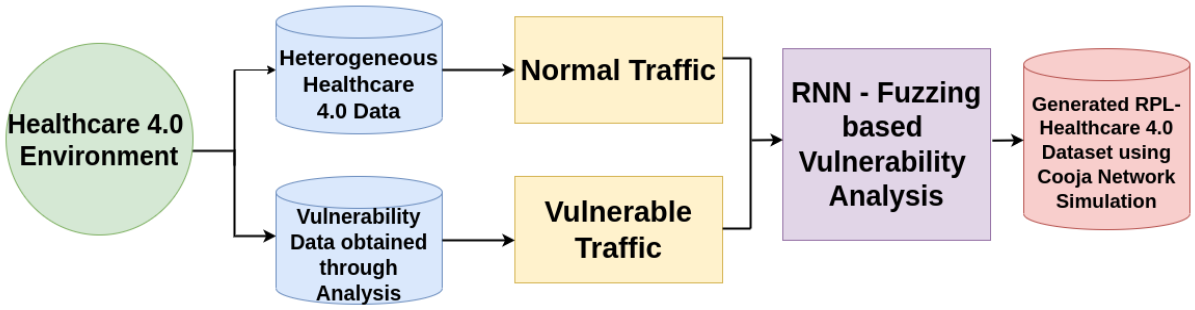


Figure. 3 RPL-Healthcare 4.0 fuzzed dataset generation

misunderstandings. Moreover, the proposed vulnerability analysis model adjusts the parameters of the RNN and fine-tunes the structure of the fuzzing output generation. Thus, it also fine-tunes the similarities between the fuzzing test cases and adjusts the legal healthcare 4.0 raw input data as vulnerability-rich data by generating different unknown behaviors. The designing process of the RNN-fuzzing model includes four main steps: determination of the target system, determination of raw RPL-healthcare 4.0 inputs, RNN-fuzzing-based vulnerability analysis, and vulnerability-rich fuzzed output data. RNN-fuzzing is a deep neural network fuzzing model that exploits multiple layers of deep learning strategy to generate the output fuzzing RPL-healthcare 4.0 data. The RNN strategy for fuzzing bypasses the constructing protocol specification process of fuzzing by improving the automata level, and thus, it reduces the workload. It does not produce logic errors or human negligence, which are majorly caused by protocol specification misunderstandings. Moreover, the proposed vulnerability analysis model adjusts the parameters of the RNN and fine-tunes the structure of the fuzzing output generation. Thus, it also fine-tunes the similarities between the fuzzing test cases and adjusts the legal healthcare 4.0 raw input data as vulnerability-rich data by generating different unknown behaviors. The designing process of the RNN-fuzzing model includes four main steps: determination of the target system, determination of raw RPL-healthcare 4.0 inputs, RNN-fuzzing-based vulnerability analysis, and vulnerability-rich fuzzed output data.

Step 1: Determination of target system

In this step, the RNN-fuzzing determines its target system, RPL-healthcare 4.0. The proposed FRVA executes RNN-fuzzing at the edges of the healthcare 4.0 architecture. It effectively handles the resource restriction issues of healthcare 4.0 devices in the device layer. After determining the target entity, the FRVA initiates the RNN-fuzzing process.

Table 2. Features of RPL-Healthcare 4.0 dataset

Sl no	Feature Name	Notations
1	Identity of Healthcare 4.0 devices	Device_Id
2	Source Identity	S_ID
3	Destination Identity	D_ID
4	Type of the Device	DT
5	Type of the Packet	Packet
6	Rank Value	R
7	Version Number	VN
8	Packet Sending Time	T_{PS}
9	Energy Consumption Level	ECL
10	Sending Rate	SR
11	Time Difference	TD
12	Number of Sending Packets	Ns
13	Number of Received Packets	N_R
14	Packet Dropping Count	PDC
15	New Fields	NF
16	Day Value for Attacks	For instance, zero

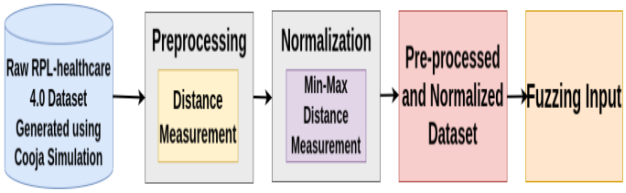


Figure. 4 Preprocessing and normalization

Step 2: Determination of raw RPL-Healthcare 4.0 fuzzing input

The legitimate and malicious Healthcare 4.0 devices are simulated with the Contiki NG platform and generate the normal and vulnerable traffic patterns for Healthcare 4.0. The features of the constructed RPL-healthcare 4.0 dataset are listed in Table 2.

Dataset preprocessing and normalization: After generating the raw RPL-Healthcare 4.0 dataset, the RNN-fuzzing considers the raw data as its input

for analysis. The raw dataset consists of normal and different attack-related information. The RNN-fuzzing exploits the generated raw RPL-healthcare 4.0 dataset for vulnerability analysis with data preprocessing and feature normalization initialization. The preprocessing starts with the RPL data cleaning and normalizing the features by filtering the relevant features. A few features in the constructed dataset are number and version consisting of a wide range of values. The data normalization process is applied to scale the normalized range from their wider range. The proposed model employs the min-max normalization method to normalize the feature values in the RPL-healthcare 4.0 dataset, as shown in Fig. 4. Consequently, the preprocessed and normalized data is input for RNN-fuzzing-based vulnerability analysis.

Step 3: RNN-fuzzing-based vulnerability analysis

The proposed fuzzing model integrates the RNN deep learning structure to analyze the vulnerabilities, as shown in Fig. 5. The deep learning model can produce accurate vulnerability analysis output data and improve the learning efficiency of the RPL-Healthcare 4.0 attack detection algorithm. Initially, the Fuzzing model takes the preprocessed and normalized dataset as its input for vulnerability analysis, which is also the input of the RNN model. The RNN model comprises three different layers according to the nature of neural networks: input, hidden, and output. The RNN input layer consists of i input units, represented as a sequence of vectors with different time t that are x (t) {x1, x2, ..., xi). As per the RNN structure, the n numbers of input units are fully connected and are connected with the j number of hidden units in the hidden layer in which the weighting metric is used to define the hidden units. The hidden layer is represented as h (t) = (h1, h2, ..., hj). Hence, the hidden layers utilize recurrent connections to establish connections. The proposed model exploits small non-zero elements to initialize the hidden units that can enhance the entire performance and network stability. The proposed RNN model utilizes rectified linear units (ReLU) as an activation function for hidden layers. Consequently, the hidden layer exploits recurrent connections to establish the connection with the output layer. The output layer comprises k numbers of units and is represented as y(t) = (y1, y2, ..., yk). The RNN model exploits the sigmoid and tan h functions as activation of the output layer between 0 and 1. Finally, the RNN fuzzing computes the output y(t) using the following Eq. (1).

$$y(t) = \max(\sigma(x), 0) \tag{1}$$

Where,

$$\sigma(x) = f_o\left(\left(\tanh\left(\frac{x}{2}\right) + 1\right)/2\right) + b_0 \tag{2}$$

In Eq. (2), the term $\sigma(x)$ is the sigmoid activation function, and the term f_o represents the tanh activation functions of RNN. The term b_0 is the bias value. By adjusting the hidden layer number for the fuzzing input dataset size, the proposed RNN fuzzing minimizes the computational complexity with minimum or acceptable overhead.

Step 4: Vulnerability-rich fuzzed output data

The RNN-fuzzing can analyze and determine the security vulnerabilities in RPL-healthcare 4.0 by feeding a large amount of unexpected input to the attack detection model. The final stage of RNN fuzzing is vulnerability-rich output generation. The proposed FRVA intends to identify eight types of vulnerabilities: rank, version number, OF, Sybil, worst parent, DoS, zero-day, and novel attacks. The CNN algorithm starts the feature selection based on the vulnerability-rich fuzzed output data. The CNN algorithm selects the attack-rich features like OF, rank, version number, and random zero-attack values from the fuzzed output data. Finally, it feeds the CNN-based feature-selected dataset to the FL-CNN-LSTM-based attack detection model.

4.2 FL-CNN-LSTM-based attack detection

Healthcare 4.0 comprises different smart sensing devices to obtain the healthcare 4.0 information of patients. Further, they report the information to the cloud server via edges. Hence, the devices are limited in power, memory, and bandwidth, whereas the edges have adequate resources compared to the devices. To manage the constrained resources of network devices effectively, the proposed model only executes the FL-CNN-LSTM-based attack detection at the edge of healthcare 4.0 devices. To elaborate on the efficiency of the attack detection model, the proposed work utilizes the globally shared parameters of the FL model to optimize the customized learning parameters of the local models of edges. Hence, the edges generate the local models using CNN-LSTM deep learning algorithms.

4.2.1. CNN-LSTM-based LM generation

The proposed model selects the CNN-LSTM combination of deep learning strategy to attack detection. The CNN is highly suitable for extracting

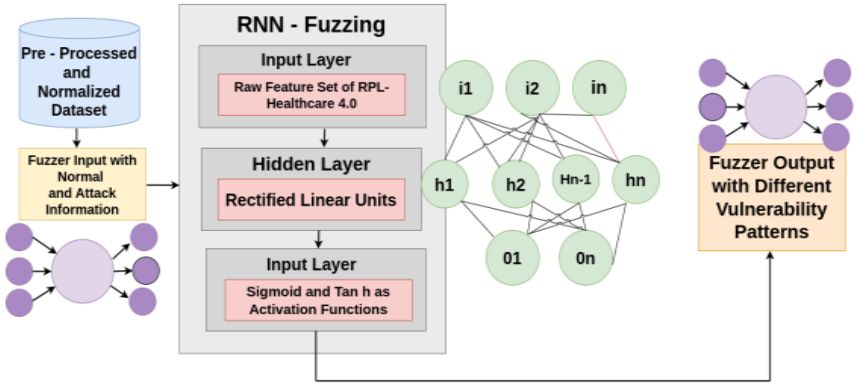


Figure. 5 RNN-fuzzing vulnerability analysis

Algorithm 1 LM generation using CNN-LSTM

//LM Generation//
Input: Local datasets of edges
Output: n number of LMs for FL aggregation
Each **edge do {**
Construct the sub dataset obtained in its area;
Initialize the CNN-LSTM learning process;
CNN **do {**
Parameter learning with local dataset (d)

multiple hidden layers;
Generate the output to the corresponding

Feeds the output to hybrid learning model;
}
LSTM **do {**
Learns the parameters in the dataset using
s subnets and gate controllers;
Generates the n number outputs;
Feeds the output to hybrid learning;
CNN-LSTM **do {**
Consolidates the outputs of CNN and
LSTM to generate the final output;
n

RPL attack-rich data features, and the LSTM is suitable for processing the time series data. Thus, it effectively rectifies the dependency between time-series data and enhances the attack detection accuracy. The proposed model consolidates the advantages of the two deep learning algorithms in attack detection.

Firstly, the CNN algorithm can learn the vulnerability-rich features better and improve the attack detection accuracy compared with conventional feature selection models. The CNN model is more appropriate for large-scale healthcare 4.0 environments. The structure of CNN is divided into three layers: convolution, pooling, and fully connected. The primary functionality of the convolution layer is to extract the salient features from RPL-healthcare 4.0, and the pooling layer samples the features. Finally, the fully connected layer connects the extracted features and obtains the final classification results. Secondly, the LSTM is an enhanced recurrent neural network (RNN) method that intends to rectify the explosion gradient problem of RPL-healthcare 4.0. Compared with the conventional RNN algorithm, LSTM exploits a wider set of gate functions to mitigate feedback and minimize short-term errors. The process of LSTM is shown in the figure in which the LSTM abstracts into four subnets: p-net, g-net, f-net, and q-net. Such subnets are a collection of gate controllers and a link to the memory component. The vector size x (t), which intimates the present learning state, controls the input and output of LSTM. Moreover, the CNN-LSTM combination has the ability to express both temporal and spatial information. Moreover, the proposed model utilizes the combination of CNN-LSTM to generate the local models, which are the initial learning output values of the learning algorithms at the edges.

Each edge device generates its initial local models for its local dataset through the CNN-LSTM learning process. The edge devices have a dataset that is a subset of the constructed RPL-healthcare 4.0 dataset. They initialize the local learning process by exploiting the local dataset of edge devices 1 to n. Hence, n number of local models are generated through CNN-LSTM. The initial learning outputs of CNN and LSTM algorithms are combined to generate the final LM of the edge. The local model generation process is explained in the figure.

4.2.2. Contextual weighted aggregation-based global model generation

Consequently, each edge updates its local model

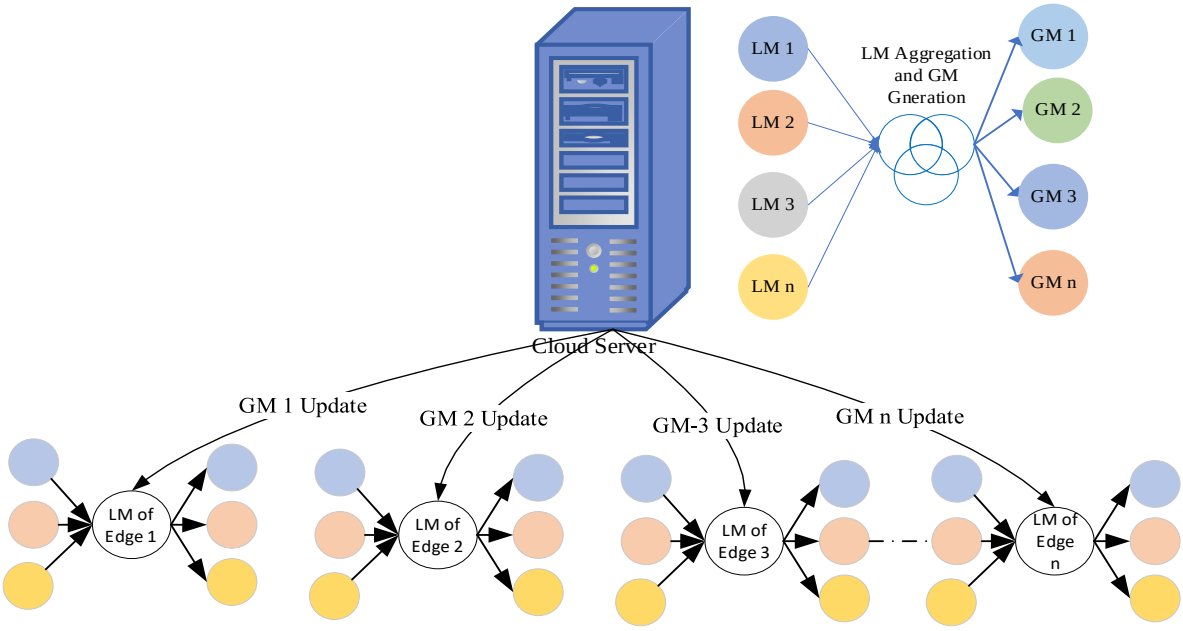


Figure. 6 GM generation process of FRVA

to the cloud server for aggregated global model generation. Each device has a context value obtained according to its behaviours. The initial context value of each edge is one. After some rounds, the context value is increased or decreased according to the behavior and resource consumption rates of edges. The local model update process is shown in the following algorithm 1. After receiving the global models of n edges, the cloud server initiates the initial global model generation process.

The proposed work generates the global shared model with the assistance of the contextual weighted aggregation model. Initially, the cloud server receives different local models (LMs) of various RPL-healthcare 4.0 edges. The weighted aggregation model provides different importance of weights to the LMs of each edge. Hence, each edge has an initial context value of 1. Consequently, according to local model updating behaviors, each edge receives various importance values. Therefore, the weighted aggregation model computes the contextual values using the standard importance degree of each edge in the hospital scenario. Further, it generates the global model using weighted aggregation. The global model generation process of the cloud server is shown in the following Fig. 6 and algorithm 2.

The local model of the edges receives high weights if the edge has many attack patterns. Hence, the cloud server aggregates the LMs by considering the contextual weights of edges. The central server receives different LM updates from n number edges in the figure, represented as LM= {LM1, LM2, LM3,…..LMn}. Further, it applies the weighted

Algorithm 2 GM generation process

//GM Generation//

Input: Local datasets of high-context edges

Output: GM generation using weighted aggregation FL model

Each **edge do {**

Feeds Gt as a LM input to cloud server;

Cloud server do {

Assigns weights to each edge based on its behaviour and resource level;

For each (LM=n; n=1, n++) {

$GM = \sum_{LM=1}^{n} (C_w)_{LM_n} * E_{LM_n}$;

Generates the GM with different attack patterns;

Feeds the GMs to each edge ;

}};

aggregation on LM to generate the global model GM= {GM1, GM2, GM3,…GMn}. The proposed model exploits the following Eq. (3) to local model aggregation at the cloud server.

$$GM = \sum_{LM=1}^{n} (C_w)_{LM_n} * E_{LM_n} \quad (3)$$

In Eq. (3), the term GM represents the global model generated at the cloud server. The term $(C_w)_{LM_n}$ refers to the contextual weighting value of edge n and the term E_{LM_n} represents the local model of edge n. Using this equation, the proposed model combines the local models of different edges without increasing the computational complexity and overhead in the network. Finally, the global models are shared to the edges, as shown in Fig. 6.

Algorithm 3 Attack detection process using FL hybrid deep learning

Attack **Detection**\\
Input: Cooja based Simulated RPL-Healthcare 4.0 Dataset
Output: Attack detection
Edges **do {**
Initiates the CNN-LSTM local learning using its local dataset;
Generates the corresponding LM;
Updates the LM to the cloud server;
LM (LM==n, n=1; n++)
Cloud server **do {**
$GM = \sum_{LM=1}^{n} (C_w)_{LM_n} * E_{LM_n}$;
Aggregates the LMs using contextual weighted aggregation;
Generates the GM with wider attack patterns;
Sends the GMs to the Edges;
};
Customize the LMs using novel attack patterns;
Improves the attack detection accuracy;
Achieves the Θ
};

4.2.3. Attack detection

Utilizing the globally shared knowledge of the cloud server, the proposed work customizes the initial local learning parameters of CNN-LSTM at each edge. The global model comprises different attack patterns of various edges. Hence, the proposed model effectively utilizes the vulnerability analysis knowledge obtained at different edges to detect the vulnerabilities in distributed edges without impacting privacy and network performance. Thus, it increases the local learning accuracy of deep learning strategies through a distributed FL model. Moreover, the edges detect the vulnerabilities and classify them under different classes based on the local learning knowledge of CNN-LSTM. The following algorithm 3 explains the vulnerability detection process of the proposed model.

5. Performance evaluation

The FRVA exploits Python libraries and Contiki NG-based simulation to analyze its effectiveness. The personal computer with Intel i5 2.5GHZ CPU and 8 GB memory is utilized to experiment. The FRVA builds the RPL-Healthcare 4.0 dataset, constructed using the attack and normal data obtained through analysis. Further, it is used for learning and attack detection using CNN-LSTM at the edges. The Contiki is highly fit to simulate the healthcare environment, as it is a reliable and widely used open-source network simulator that enables internet connections between tiny minimum-cost and low-power medical sensing devices. It also provides support to the RPL protocol for low-power IPv6 networking. Moreover, the proposed FRVA analyzes the efficacy of the vulnerability detection model with a hybrid CNN-LSTM deep learning strategy by comparing it with various existing algorithms such as federated semi-supervised learning (FSSL) [24] and FL based anomaly detection (FLAD) [29]. It also compares with baseline learning algorithms that are LSTM [32], CNN, ANN [33], MLP [34], simple-RNN (S-RNN) [32], logistic-reg (L-Reg) [35], naive-bias (NV), and KNN.The simulation parameters of FRVA are shown in the following Table 3.

Table 3. Simulation parameters of FRVA

Parameter	Values
Simulator	Contiki NG
Protocol	RPL-Healthcare 4.0
Fuzzing Model	RNN-Fuzzing
Deep Learning Model	Hybrid with CNN and LSTM
Dataset	RHD
Simulation Area	500m*500m
Number of Nodes	50
Number of Edges	5
Physical Layer	IEEE 802.15.4
Radio Medium	UDGM
Transmission Range	50 m
Simulation Time	5 Minutes

5.1 Performance metrics:

The effectiveness of the proposed FRVA is analysed in terms of various performance metrics, which are as follows.

Accuracy: It is the percentage of attackers that are correctly identified as attackers.

$$\text{Accuracy} = \frac{\text{Number of correctly identified attackers}}{\text{total number of attackers}} * 100$$

Precision: It is the percentage of correctly identified attacks.

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

TP-true positive, FP-false positive

Recall: It is the percentage of correct positive attack detection to the total number of attackers.

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

FN-false negative

F1-Score: It is the combination of precision and recall. The F-score is calculated by taking harmonic mean to precision and recall.

$$\text{F1} - \text{Score} = \frac{\text{TP}}{\text{TP}+\frac{1}{2}(\text{FP+FN})}$$

Specificity: It is the ratio of true negatives to the summation of true negatives and false positives.

$$\text{Specificity} = \frac{\text{TN}}{\text{TN+FP}}$$

TN-true negative

MAE: It is the summation of the exact difference between actual and observed values of attack detection.

AUC-Score: It represents the probability that is estimated using the trapezoidal rule.

Log-Loss: It represents a cross-entropy loss value computed using the actual and identified values of attackers.

5.2 Simulation results

The simulation results are presented for the FL-based hybrid learning models.

5.2.1. Contiki NG-based attack dataset generation and Labeling

Initially, the proposed FRVA utilizes the Contiki NG simulator to gather the data from the healthcare 4.0 environment and construct the raw RPL-healthcare 4.0 with eight vulnerabilities. During network initialization, by running the RPL-healthcare 4.0 code Contiki NG, the proposed FRVA gathers the RPL traces as raw packet capture (PCAP) files from the I4.0 environment. To conduct experimental evaluation and generate the dataset with normal and attack information, the FRVA conducts Contiki NG-based simulations. The FRVA system considers Eight different RPL-healthcare topologies with 50 wireless healthcare devices, in which sixteen devices (32% of total density) are considered attackers. Each topology comprises different attacker devices. Among 32% of attackers over 50 devices topology, every 2% represents the rank, version number, OF, Sybil, worst parent, DoS, zero-day, and novel. Algorithm 4 explains the different dataset conditions to label such eight attacks.

5.2.2. Deep learning results

Table 4 demonstrates the performance comparison results of various deep learning algorithms like hybrid, FSSL, FLAD, LSTM, CNN, ANN, MLP, S-RNN, L-Reg, NB, and KNN.

Fig. 7 illustrates the accuracy, precision, recall, F1-core, and sensitivity results of various hybrid deep learning algorithms, FSSL, FLAD, LSTM, CNN, ANN, MLP, S-RNN, and L-Reg. The results show that the proposed hybrid CNN-LSTM model improves the detection accuracy than the other FL models, that are FSSL, FLAD and single baseline deep learning models such as LSTM, CNN, ANN, MLP, S-RNN, L-Reg, NB, and KNN. The main reason behind this is that the proposed hybrid deep learning model combines the results of CNN and LSTM in attack detection, thereby reducing false positives and error rates. In addition, the FRVA considers the NGFL concept to be precise customized learning models in every healthcare 4.0 environment. Optimizing the local learning models by exploiting the advantage of the FL global model maximizes the learning accuracy significantly and enhances the attack detection accuracy of the hybrid model in FRVA. For instance, the FL-enabled hybrid model improves the accuracy by 25.83% and 5.97% than the existing FL-based attack detection models like FSSL and FLAD, respectively. Unlike the proposed FRVA, the existing FSSL and FLVA exploit baseline algorithms for attack detection. Thus, it leads to minimizing the accuracy due to learning errors. Furthermore, the proposed FRVA shows superior results compared to single baseline models. The reason is that the hybrid models take the attack detection decisions by considering the outputs of two various learning strategies, resulting in high accuracy. For example, the proposed FL-base hybrid CNN-LSTM combinations improve accuracy by 5.55% and 12.9% compared to the baseline LSTM and CNN algorithms.

Similarly, the proposed hybrid FRVA improves the precision values by 5.69%, 12.33%, and 7.61% compared to the fundamental LSTM, CNN, and MLP algorithms. Unlike the two existing models,

Table 4. Performance results comparison of hybrid model

Metrics	Hybrid	FSSL	FLAD	LSTM	CNN	ANN	MLP	S-RNN	L-Reg	NB	KNN
Accuracy (%)	98.19	72.36	92.22	92.64	85.29	84.44	90.38	86.14	75.25	75.54	72.83
Precision (%)	98.31	70.3	91.97	92.62	85.98	85.46	90.7	85.58	79.88	73.56	85.69
Recall (%)	98.02	75.15	92.83	92.36	84.17	77.55	86.63	81.34	61.71	65.28	56.7
F1-Score (%)	98.15	70.53	92.11	92.48	84.7	79.94	88.28	82.96	61.8	66.54	53.57
Specificity (%)	97.9	73.11	92.29	91.6	83.25	75.6	84.2	79.4	60.2	63.1	54.8
MAE	0.018	0.276	0.078	0.074	0.147	0.155	0.096	0.139	0.248	0.245	0.272
AUC-Score	98.02	73.11	92.29	92.36	84.17	77.55	86.63	81.34	61.71	65.28	56.7
Log-Loss	0.6504	9.9621	2.8052	2.6525	5.2994	5.6058	3.4651	4.9931	8.092	8.8159	9.792

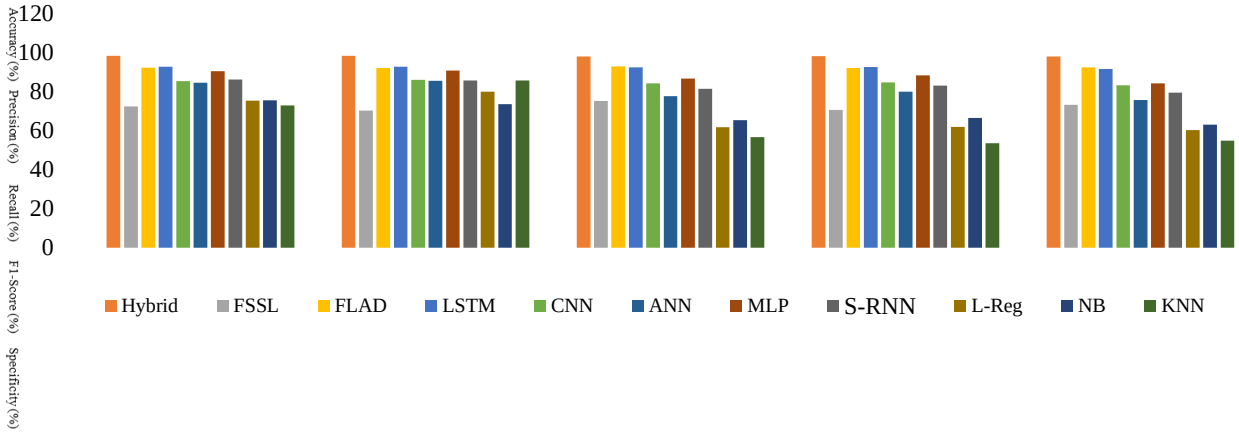
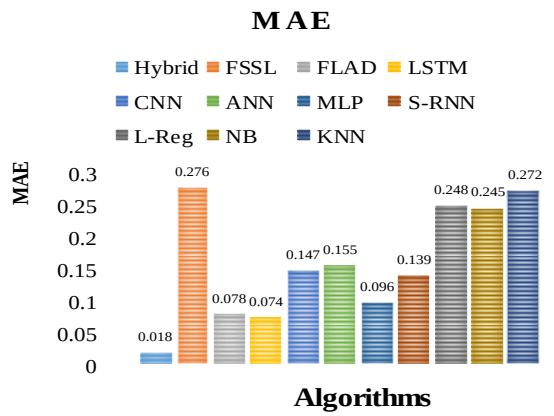


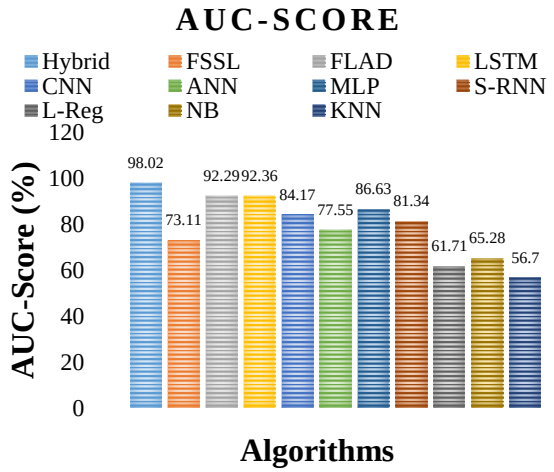
Figure. 7 Performance results of different algorithms

the proposed FRVA combines the results of CNN and LSTM in making attack detection decisions and improves detection accuracy. The FSSL and FLAD comprise single learning models, resulting in minimum recall values. For example, the proposed hybrid model enhances the recall by 22.87% and 5.19% than the existing FSSL and FLAD, respectively. The high precision and recall results obtained by the proposed model also improve the F1-Score and sensitivity value. The proposed FRVA neglects such an issue by including the hybrid learning strategy in which the attack detection decisions are taken using different learning results. Also, the attack detection decision-making with a hybrid model enhances the specificity of the single baseline models like CNN and LSTM. Thus, it also assists in maximizing the sensitivity. For instance, the proposed hybrid model improves the F1-score by 5.67% and 13.45% compared to the single LSTM and CNN models. Also, the proposed hybrid models enhance the specificity by 22.3% and 34.8% than the baseline ANN and NB algorithms, respectively.

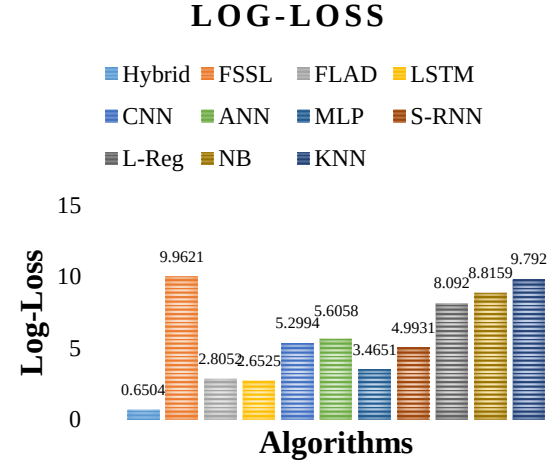
Fig. 8 illustrates the MAE, AUC-score, and log-loss comparison results of different deep learning algorithms. The MAE is obtained by taking the average to the absolute error values produced by the deep learning models. Compared with existing FSSL and FLAD, the proposed hybrid CNN-LSTM minimizes the MAE in attack detection by incorporating the advantages of CNN fuzzing-based vulnerability analysis, FL-based customized local model update, and hybrid deep learning-based attack detection, as shown in Fig. 8 (a). The vulnerability analysis improves the novel attack distributions in the learning dataset, and the hybrid model minimizes the error rates in detection. For instance, the hybrid, FSSL, and FLAD obtain 0.018, 0.276, and 0.078 MAE values, respectively. By taking the attack detection decision using two deep learning algorithms like CNN and LSTM, the proposed



(a)



(b)



(c)

Figure. 8: (a) Algorithms Vs MAE, (b) Algorithms Vs AUC score, and (c) Algorithms Vs log loss

FRVA also shows its superiority over the baseline learning models. For example, the MAE error rates of hybrid FRVA, LSTM, and CNN are 0.018, 0.074, and 0.147, respectively. Also, the advantages of using fuzzing vulnerability analysis, FL-based distributed learning, and hybrid deep learning-based attack detection improve the AUC-Score of the proposed model when compared with baseline algorithms, as demonstrated in Fig. 8 (b). The reason is that the high attack pattern distribution and the attack decision-making with the hybrid learning strategy diminish errors, resulting in AUC-Score values enhancement. For example, the proposed hybrid CNN-LSTM improves the AUC-Score by 5.66%, 13.85%, 11.39%, and 41.32% than the LSTM, CNN, MLP, and KNN, respectively. Consequently, Fig. 8 (c) shows that the log-loss value of the proposed hybrid FRVA is minimal compared to other existing FSSL and FLAD models. Compared with FSSL and FLAD, the FRVA includes the vulnerability analysis that enhances the learning efficiency of the hybrid FRVA. Thus, the proposed model minimizes the log-loss effectively. The vulnerability analysis also improves the learning accuracy by distributing large attack patterns. For example, the Log-loss values of hybrid, FSSL, and FLAD are 0.6504, 9.9621, and 2.8052, respectively.

6. Conclusion

This paper proposes a security framework, FRVA, to defend against multiple RPL-healthcare 4.0 attacks. By integrating the RNN-fuzzing-based vulnerability analysis and FL-enabled CNN-LSTM-based attack detection, the FRVA improves security without impacting the RPL-healthcare 4.0 performance. The proposed FRVA improves security against eight attacks by considering the fuzzed output data and FL-based global parameters. Moreover, the execution of vulnerability analysis and attack detection at edges manages the network resources efficiently and prologs the network lifetime. Finally, the Python-based simulation results show the superiority of hybrid CNN-LSTM in terms of different performance metrics. The simulation results prove that the proposed FRVA accomplishes superior detection accuracy by 5.55% and 12.9%, respectively than the baseline CNN and LSTM methods. The accuracy of FRVA also improves by 25.83% and 5.97% when compared with existing FSSL and FLAD.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

“Conceptualization, K. Kowsalyadevi and N.V, Balaji; methodology, K. Kowsalyadevi; software, K.

Kowsalyadevi; validation, K. Kowsalyadevi, and N. V, Balaji; formal analysis, K. Kowsalyadevi; investigation, N. V, Balaji; resources, K. Kowsalyadevi; data curation, N. V, Balaji; writing—original draft preparation, K. Kowsalyadevi; writing—review and editing, K. Kowsalyadevi; visualization, N. V, Balaji; supervision, N. V, Balaji; project administration, N. V, Balaji; funding acquisition, K. Kowsalyadevi".

References

[1] S. Paul, M. Riffat, A. Yasir, M. N. Mahim, B. Y. Sharnali, I. T. Naheen, A. Rahman, and A. Kulkarni, "Industry 4.0 applications for medical/healthcare services", *Journal of Sensor and Actuator Network*, Vol. 10, No. 3, pp. 43, 2021.

[2] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Medical 4.0 technologies for healthcare: Features, capabilities, and applications", *Internet of Things and Cyber-Physical Systems*, Vol. 2, pp. 12–30, 2022.

[3] Kharrufa, H. A. A. A. Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A review", *Journal of IEEE Sensor*, Vol. 19, No. 15, pp. 5952–5967, 2019.

[4] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, No. 1, pp. 361–407, 2023.

[5] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, No. 1, pp. 361–407, 2023.

[6] A. Clim, "Cyber security beyond the industry 4.0 era. A short review on a few technological promises", *Informatica Economica*, Vol. 23, No. 2, pp. 34–44, 2019.

[7] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the internet of things: A review", *IEEE Sensor Journal*, Vol. 20, No. 11, pp. 5666–5690, 2020.

[8] Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, "Intrusion detection systems in RPL-based 6LoWPAN: A systematic literature review", *IEEE Sensor Journal*, Vol. 21, No. 11, pp. 12940–12968, 2021.

[9] T. A. A. Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and Deep Learning approaches for detecting attacks in RPL-based 6LoWPAN of internet of things", *Sensors (Basel)*, Vol. 22, No. 9, 2022.

[10] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey", *IEEE Communication Survey and Tutorial*, Vol. 23, No. 3, pp. 1622–1658, 2021.

[11] E. M. Campos, P. F. Saura, A. G. Vidal, J. L. H. Ramos, J. B. Bernabe, G. Baldini, and A. Skarmeta, "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges", *Computer Network*, Vol. 203, No. 108661, 2022.

[12] Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things", *IEEE Internet Things Journal*, Vol. 6, No. 4, pp. 6822–6834, 2019.

[13] S. O. M. Kamel, E. R. Institute, Cairo, Egypt, and S. A. Elhamayed, "Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network", *Int. J. Comput. Netw. Inf. Secur.*, Vol. 12, No. 4, pp. 11–29, 2020.

[14] Dogan, S. Yilmaz, and S. Sen, "Analysis of RPL objective functions with security perspective", In: *Proc of the 11th International Conference on Sensor Networks*, pp. 71-80, 2022.

[15] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. A. Zain, "Rank and wormhole attack detection model for RPL-based internet of things using machine learning", *Sensors (Basel)*, Vol. 22, No. 18, p. 6765, 2022.

[16] M. Pishdar, Y. Seifi, M. Nasiri, and M. B. Mohammadi, "PCC-RPL: An efficient trust-based security extension for RPL", *Inf. Secur. J. Glob. Perspect.*, Vol. 31, No. 2, pp. 168–178, 2022.

[17] G. Casteur, A. Aubaret, B. Blondeau, V. Clouet, A. Quemat, V. Pical, and R. Zitouni, "Fuzzing attacks for vulnerability discovery within MQTT protocol", In: *Proc. of 2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020.

[18] S. Kim, J. Cho, C. Lee, and T. Shon, "Smart seed selection-based effective black box fuzzing for IIoT protocol", *J. Supercomput.*, Vol. 76, No. 12, pp. 10140–10154, 2020.

[19] P. Sharma, T. Sakthivel, and I. K. Alnajjar, "Optimized Federated Learning with Ensemble

of Sequential Models for Detecting RPL Routing Attacks for AMI Networks", *Research Square*, Vol. 21, 2023, doi: 10.21203/rs.3.rs-2571557/v1.

[20] W. Schneble and T. Geethapriya, "Attack detection using federated learning in medical cyber-physical systems", In: *Proc. of 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vol. 29, pp. 1-8. 2019.

[21] N. Abosata, S. A. Rubaye, and G. Inalhan, "Customised intrusion detection for an industrial IoT heterogeneous network based on machine learning algorithms called FTL-CID", *Sensors (Basel)*, Vol. 23, No. 1, 2022.

[22] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices", *IEEE Internet Things J.*, Vol. 9, No. 5, pp. 3930–3944, 2022.

[23] B. Li, S. Chen, and Z. Peng, "New generation federated learning", *Sensors (Basel)*, Vol. 22, No. 21, p. 8475, 2022.

[24] Rajagopal, S. M. Rajagopal, M. Supriya, and R. Buyya. "FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge-Fog-Cloud computing environments", *Internet of Things*, Vol. 22, No. 100784, 2023.

[25] Z. Jin, Z. Liang, M. He, Y. Peng, H. Xue, and Y. Wang, "A federated semi-supervised learning approach for network traffic classification", *Int. J. Netw. Manage.*, Vol. 33, No. 3, 2023.

[26] A. Tabassum, A. Erbad, W. Lebda, A. Mohamed, and M. Guizani, "FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning", *Comput. Commun.*, Vol. 192, pp. 299–310, 2022.

[27] A. Wijesinghe, S. Zhang, and Z. Ding, "PS-FedGAN: An efficient federated learning framework based on partially shared generative adversarial networks for data privacy", *ArXiv [cs.LG]*, 2023.

[28] Mugunthan, V. Gokul, L. Kagal, and S. Dubnov, "Bias-Free FedGAN: A federated approach to generate bias-free datasets", *ArXiv [cs.LG]*, 2021.

[29] S. Duan, C. Liu, P. Han, X. Jin, X. Zhang, T. He, H. Pan, and X. Xiang, "HT-Fed-GAN: Federated Generative Model for Decentralized Tabular Data Synthesis", *Entropy*, Vol. 25, No. 1, 2022.

[30] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks", *IEEE Internet Things J.*, Vol. 9, No. 4, pp. 2545–2554, 2022.

[31] W. W. Wang, X. Li, X. Qiu, X. Zhang, V. Brusic, and J. Zhao, "A privacy preserving framework for federated learning in smart healthcare systems", *Inf. Process. Manag.*, Vol. 60, No. 1, p. 103167, 2023.

[32] C. Briggs, Z. Fan, and P. Andras, "A review of privacy-preserving federated learning for the internet-of-things", *Federated Learning Systems, Cham: Springer International Publishing*, pp. 21–50, 2021.

[33] S. A. Kustrin and R. Beresford, "Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research", *Journal of Pharmaceutical and Biomedical Analysis*, Vol. 22, No. 5, pp. 717-727, 2000.

[34] H. Taud, and J. F. Mas, "Multilayer perceptron (MLP)", *Geomatic Approaches for Modeling Land Change Scenarios*, pp. 451-455, 2018.

[35] A. Das, "Logistic regression. In Encyclopedia of Quality of Life and Well-Being Research", *Cham: Springer International Publishing*, pp. 1-2, 2021.