Intelligent and Secure Detection of Cyber-attacks in Industrial Internet of Things: A Federated Learning Framework

Ahmed Sleem

Thebes Higher Institute for Computer and Administrative Sciences, Egypt
Ministry of communication and information technology, Egypt
Email: Ahmedsleem8000@gmail.com ; asleem@mcit.gov.eg

Abstract

The increasing integration of traditional industrial systems with smart networking and communications technology (such as fifth-generation networks, software-defined networking, and digital twin), has drastically widened the security vulnerabilities of the industrial internet of things (IIoT). Nevertheless, owing to the lack of sufficient instances of high-quality attacks, it has been incredibly difficult to resist the cyberattacks that directed at such a substantial, complicated, and dynamic IIoT. This work introduces an intelligent federated deep learning framework, termed FED-SEC, for automatic and early identification of cyber-attacks against IIoT infrastructure. In particular, a new convolutional recurrent network designed to detect cyberattacks within IIoT data. Then, a secure federated learning scheme presented to promote making use of mobile edge computing to enable the distributed IIoT entities to cooperate together to train a unified model for cyberattack detection in a privacy-preserved manner. More, a safe communication channel constructed via an improved Homomorphic Encryption scheme aiming to keep the model parameters secure against any leakage of inferential attacks, especially throughout the training procedure. Massive experimentations on multiple public datasets of IIoT cyberattacks proved the high-level efficacy of the FED-SEC in discovering different categories of cyber-attacks against IIoT and the superiorities over cutting-edge approaches.

Keywords: Internet of Things (IoT); Mobile Edge Computing; Federated Learning; cyberattack detection; Deep Learning

1. Introduction

The Industrial Internet of Things (IIoT) refers to the integration of high-tech sensors and actuators into production and processing facilities. IIoT also referred to as the industrial internet or Industry 4.0, takes advantage of the information that "dumb machines" have been producing in industrial settings for years by employing the power of smart machines and real-time analytics. The underlying principle of IIoT is that intelligent robots are superior to people in acquiring and evaluating data in real time, as well as in conveying crucial information that can speed up and improve the quality of business choices. Companies can save time and money thanks to the increased accuracy and timeliness of alerts provided by connected sensors and actuators, which can lend a hand to business intelligence initiatives. the overarching structure of an IIoT system is encased in intelligent networking (such as fifth generation (5G), beyond 5G (B5G), Software Defined Networks (SDN), network function virtualization (NVF), etc.) and computational paradigms like cloud computing, fog computing, edge computing, etc.

IIoT has the potential to improve quality control, environmentally friendly and sustainable practices, supply chain traceability, and delivery capabilities in the industrial sector. IIoT is essential in an industrial context for Predictive maintenance, improved customer support, power management, and remote monitoring. Unlike the IoT, which mostly refers to consumer electronics and the networking of physical objects, the IIoT focused on industrial applications. Its uniqueness lies in the fact that it bridges the gap between information technology and operational technologies, which comprise the industrial control systems (ICSs) (such as programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), distributed control systems (DCSs)).

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

Although it is easy to understand the benefits of IIoT, it is also important to note that these technological developments have not been made without risk. Traditional manufacturing systems have been built with inadequate security procedures, which has resulted in a large number of potentially exploitable holes being left unpatched. The swift combination of innovative communication networks and computational technologies has significantly expanded the attack surface by presenting new flaws that can be used across software-based endpoints, connections, implementations, and cloud services. This has resulted in a significant increase in the number of potential targets for malicious actors. One notable security breach occurred in December 2015 when BlackEnergy malware was used in a cyberattack on Ukraine's power infrastructure, cutting electricity to more than 30 substations and leaving over 230 thousand people without power for one to six hours. Notable cyber incidents relating to IIoT include the Stuxnet attack on countries' critical industries such as the weapon industry, mining industry, etc. These attacks show that Industrial IIoT will continue to attract attention from bad actors, especially those with state ties, for the near future. In this regard, the United States has been a strong advocate for the need for IIoT investing in cybersecurity. "Significant rise in the interconnectivity of functioning technologies over the IIoT poses other problems for the management of systems safety," as stated by the U.S. Unit of Homeland Security in the 2016 ICS-CERT in Annual Assessment Report. In another definition, cybersecurity is regarded to have a vital role in keeping the functioning of contemporary industries secure and safe [1].

There has been a growing focus on AI-relevant cyberattack detection algorithms in the state-of-the-art literature to combat cybersecurity threats to industrial control and monitoring systems in recent years. The issue of protecting IIoT systems has been the subject of numerous studies from a variety of perspectives. Regrettably, most established AI-relevant cyberattack detection strategies associated with IIoT are constructed on the premise that reasonably good instances of cyberattacks on IIoT are indeed obtainable, and easily accessible, for the system defender to construct a preferred cyberattack detection model. Nevertheless, in practice, the owner of an IIoT typically has very few attack samples to deal with, which makes the model-building task extremely difficult. In addition, due to the sensitive nature of the data involved, IIoT owners are typically hesitant to make attack samples (or even instances of "normal" behavior) available to other parties. This highlights the apparent intractable need for developing an intelligent, secure, and reliable artificial intelligence (AI) based model for detecting cyber-attacks in IIoT environments.

Despite the research efforts devoted to securing IIoT, many research gaps are still not completely fulfilled in the literature. First, the industrial data are always distributed across different industrial partners, which pose aggregating the data to a central location to be able to develop a data-driven cyber-attack detector. However, distributed learning can provide a suitable solution to this problem. Second, edge devices are known to have a limited set of resources. Third, the distributed nature of IIoT systems makes the deep learning models vulnerable to privacy leakage or reversal attacks that can shape a major challenge for the applicability or trustworthiness of cyber-attack detectors. In response to the above challenges, this work proposed a novel federated learning (FL) framework, termed FED-SEC that contributes to addressing the problem of cyber-attack detection through the following innovations:

- This paper presents a new convolutional recurrent network for automated and efficient detection of cyber-attacks in IIoT data streams. Denial-of-service (DoS), eavesdropping, response insertion, and session hijacking attacks are only some of the cyberattacks that can be effectively detected by this paradigm when applied to IIoTs.
- The FED-SEC presents a secure federated learning system, which, on the one hand, makes it possible to construct a holistic cyberattack discovery model by making use of the data resources owned by several IIoT vendors. On the contrary, side, FED-SEC allows data processing to take place on the premises of each individual IIoT, so effectively preserving the confidentiality of data resources.
- To ensure that sensitive model parameters remain private and secure throughout the training process, we devise an encrypted communication protocol for the proposed FED-SEC based on an improved Homomorphic Encryption, with intelligent encryption and decryption procedures.

The remaining part of this work is structured as follows. An analytical review of the literature is presented in Section 2. Then, the methodology of the FED-SEC is presented in Section 3. Section 4 present the experimental configuration of our study. Following, section 5 articulates the results and experimental findings. Finally, section 6 concludes this study and points out possible research directions.

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

2. Related Work

An overview of recent research on IIoT-specific cyberattack detection systems and federated learning-based cyberattack detection approaches is provided here. An overview of recent research on IIoT-specific cyberattack detection systems and FL-based cyber-attack detection approaches is provided here.

A. cyberattacks Detection in IIoT

There has been a rise in interest in studying cyber-attack detection techniques for IIoT in recent times. As an instance, the authors of [2] presented a DL-based cyber-attack recognition approach, called log-cosh conditional variational autoencoder (LCVAE). From its ancestor, the conditional variational autoencoder takes on the capability to model the intricate distributions of observed data and produce novel data in which predefined classes appear naturally. LCVAE characterized the discrete nature of the incursion data with the use of the log hyperbolic cosine (log-cosh) function. It is more efficient in generating different cyber-attack data for the unbalanced classes, it is able to create data in a way that is well-matched between generation and reconstructive processes. To enhance detection performance, a CNN-based extractor is integrated into LCVAE to fuse patterns from both real-world and synthetic cyber-attack data and then classify them. The authors of [3] developed a K-means algorithm for cyber-attack detection based on repetitive random sampling, hence called Repeated random sampling- K-means (SDRK), by combining supervised deep network with unsupervised clustering methods. Between the Internet of Things (IoT) and the cloud, you'll find the fog nodes where the cyber-attack detection and prevention algorithms live, and this is where the SDRK was put to detect the data deluge (DD) attack. Besides, the authors of [4], developed a cyber-attack detection system by combining a stacked autoencoder (AE) and a deep model, in which the former used an unsupervised learning method to narrow in the features included in the incoming network data. After that, a supervised training process is used to teach the deep network how to retrieve deep features for use in the classifier. In addition, the authors of [5], developed a lightweight deep neural network-based technique for IoT network cyber-attack detection (LNN). By employing the principle component analysis (PCA) algorithm to accomplish feature discretization in the information preprocessing step, we are able to prevent the high computational cost that would otherwise result from using high-dimensional raw traffic information. For excellent feature extraction at minimal computing cost, our classifier employs the enlargement and contraction architecture, the inverted residual formation, and the channel shuffle function.

B. Mobile Ede Computing

An edge-computing architecture typically includes a (big) number of heterogeneous IoT devices; hence the two ideas are becoming increasingly interwoven. However, this broadens the attack surface, as any one of these IoT devices can be compromised to open the door to more forms of cybercrime. For example, the authors of [6] presented a multi-tiered heterogeneous Internet of Vehicles (IoVs) network that is secured, effective, and smart and is centered on edge computing. the purpose and utility of such a design are first discussed. Then, we show how unsupervised deep learning approaches might make it easier to spot unusual driving patterns and safeguard this kind of infrastructure. The authors of [7] introduced the Passband framework, a smart IDS that can safeguard directly linked Internet of Things gadgets from cyber-attack. The suggested method is unique in that it can be implemented on inexpensive IoT gateways, making full use of the edge computing architecture to identify cyber-attacks as close as feasible to the associated data sources. More, the authors of [8] proposed to delegate cyber-attack detection activities to federated vehicle nodes located within adjacent created ad hoc vehicular fog, a fog-enabled vehicular-edge computing (VEC) approach. They have formalized it as a multicriteria model and applied an evolutionary algorithm to it, with the goal of increasing offloading durability in the context of high mobility while decreasing computing implementation energy consumption and time. Further, the authors of [9] suggested a solution to involve IIoT devices in detecting adversarial fake identities, or Sybil devices, and communicating that information to edge servers to block the upstream distribution of malicious activities. Each edge server, upon detecting a Sybil assault, runs a parallel artificial bee colony (pABC) algorithm to configure the IIoT network optimally. Depending on their storage and computing capacities, edge servers undertake job relocation to their surrounding servers for task scheduling and improved network performance.

C. Federated Cyberattack Detection

Federated learning (FL) has been identified as a potential approach for identifying data isolation questions in recent times, and it has been widely embraced in various fields. A number of academics, for instance, have lately carried out investigations based on FL to accomplish cyber-attack recognition. in this context, the authors of [1] developed DeepFed, as a federated deep learning technique for identifying cyber attacks targeting cyber-physical systems (CPSs) by integrating CNN and a GRU for distributed cyber-attack detection. The design of DeepFed enables several

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

industrial operators to work together to produce a robust cyber-attack detection model without compromising individual data privacy. The DeepFed designed with a secure communication protocol is developed relying on the Paillier cryptosystem to protect the confidentiality of model parameters during training. More, the authors of [10] proposed preemptively recognizing cyber-attack in IoT networks utilizing distributed on-device data and presented an (FL-based anomaly detection approach that applied GRUs for federated training rounds and preserves data on edge devices by transmitting just the learned weights to the FL server. Further, the ensemble component of the method combines data from several sources to fine-tune the correctness of the overall ML model. The authors of [11] developed the federated DL (FDL) technique for zero-day botnet attack recognition that classified network traffic using the effective deep network. The federated averaging (FedAvg) approach is applied to centrally collect local updates from a number of IoT-edge devices, while an aggregation server manages the training of the local models in those devices. moreover, the authors of [12] used a blur-label-flipping tactic to propose a federated backdoor filter defense that can detect malicious inputs and make the data usable again. To stop even the most sophisticated attacks from getting through, they constructed numerous filters using understandable AI models on the server and deliver them to users at arbitrary. Furthermore, the authors of [13] presented a thorough analysis of Differential Privacy (DP) methods used in the development of a FL-enabled detection of cyber-attacks in IIoT.

3. Methodology

This section provides more detail on the proposed FED-SEC framework in terms of the network model, threat model, Convolutional-LSTM as a cyber-attack detector, the detail of the federated training pipeline, and the encrypted messaging method for securing the training parameters.

3.1. Network Model

The model of the system that is being contemplated is known as a federated system, and it is composed primarily of three distinct categories of entities, namely, a trusted agency, a cloud platform, and a group of industry actors. 1) Cloud platform: The cloud server is in charge of developing a thorough cyberattack recognition model by unifying the updates of the model trained individually by each industrial client. If you want an "optimal" cyberattack detection approach, you'll need multiple iterations of communication between the cloud platform and each industrial operator. 2) Trust agency: The trusted agency is responsible for initializing the system, creating communal and isolated keys for the encrypted communication methodology based on Homomorphic Encryption, and constructing safe lines of communication between the cloud platform and each industrialized client. 3) Industrial actors: On account of the IIoT owner, each industrialized agent is responsible for developing a local model for early detection of cyber-attacks using its own gathered IIoT data and contributing to the upgrading of the gradients of the cyberattacks recognition model through frequent interaction with the cloud platform.

3.2. Threat Scheme

When developing the threat model, we took into account cyber-attacks that were directed not only at the proposed federated learning framework but also at the IIoT. First, cyber-attacks on IIoT ecosystem, in contrast to traditional computer systems, the Internet of Things (IIoT) is vulnerable to not only conventional forms of cyber-attack, like denial of service and distributed denial of service (DDoS) cyber threats, nonetheless, also a boundary of extremely specialized new forms of cyber-attack that are specifically designed to target IIoT, such as command injection and reaction injection attacks. In this study, we investigate all of the cyber risks that were discussed earlier, with a particular emphasis on the foregoing:

- The purpose of a reconnaissance assault is often to collect valuable information about IIoT, map the topologies of the network, and identify device attributes like the producer, compatible network practices, and device identifiers.
- In the field of industry 4.0, response injection attacks are typically conducted with the intention of disrupting the surveillance and exposure of the status of a distant activity. Those attacks have the potential to misrepresent responses reporting to inquiring parties, leading to the provision of skewed information regarding the state of the system.
- Injections of bogus control or configuration commands are frequently used in the launch of command injection attacks, which are designed to deceive the behaviors of IIoT systems. These kinds of attacks can result in unauthorized changes being made to the settings of devices, the setpoints of processes, or communications endpoints.

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

- DoS attacks are typically executed by bombarding their targets with unnecessary queries at a high rate. This is done to deplete the assets of computer systems in IIoT, which can either cause the services to become inoperable or inhibit queries from becoming accomplished.

Second, in Cyber-attacks targeting FL systems, in the framework for federated deep learning that is being investigated, it is taken for granted that the governing body can be completely relied upon, and the cloud server is a party that is honest in some aspects but not others. carrying out all of the assigned duties while maintaining an interest in the model components of the cyberattacks recognizer called parameters. Furthermore, it is presumed that all industrial operators are at least somewhat truthful and that they always follow the rules. the protocols that were established however might also be concerned with the data of other industrial actors. In addition to that, we do take that into account as well. Those nefarious snoopers or other outside adversaries may be listening in intercept by means of the communication channels in an effort to gain entry to the stored data of each individual IIoT, as well as the parameters regarding the model for detecting cyberattacks s. In this particular instance, we will consider the following two different kinds of online dangers:

- Listening in on data resources: with regard to the industrial proprietors of IIoT, their respective training data to make the incursion recognition network, especially cyberattack cases are extremely delicate and perhaps even crucial to the nation. If it known, with the help of the cloud server, it could result in significant business. Losses or serious threats to the country's security.
- Eavesdropping on the parameters of the model: the parameters of a vital piece of information are contained within a cyberattack detection model. Concerning the available data resources. In the event that they are accessible from the outside world in an unlawful manner, some foundational understanding pertaining to such data resources, for example, the kind of online dangers or its There is a possibility that certain example distributions will be disclosed.

3.3. Convolutional-LSTM

Here, we present the newly invented Convolutional LSTM for cyber-attack detection on the industrial actor's devices in the IIoT system.

A. Structural Design

The intended model is predominantly comprised of a convolutional block, LSTM blocks, tailed by a Feed Foreword network (FNN) module with a Softmax layer at the end. The details of each building block are given as follows:

First, convolutional parts consist of three convolutional layers, each followed by a batch normalization and a max-pooling (MP) operation. For an input x formulated as a 1D feature, the convolutional blocks calculate as follows

$$h_1 = MP\left(BN\left(Conv(x)\right)\right) \quad (1)$$

$$h_2 = MP\left(BN\left(Conv(h_1)\right)\right) \quad (2)$$

$$h_3 = MP\left(BN\left(Conv(h_2)\right)\right) \quad (3)$$

$$u = Flatten(h_3) \quad (4)$$

Second, for the LSTM part, it is composed of two indistinguishable GRU layers, the input x is regarded as a multivariate time series with one timestep. Before providing x to the LSTM blocks, a dimension shuffling operation is applied to convert the temporal dimension of the feature vector as follows:

$$\tilde{x} = \text{shuffle (x)} \quad (5)$$

Then, the LSTM layer is applied to manipulate $\tilde{x}$ in a way that enables the extraction of temporal patterns. LSTM is designed to add a *memory cell,* C_t, to save long-term temporal relations. It consists of three gating operations (*output gate,* O_t, *input gate,* I_t, *forget gate,* F_t) to control the flow of information in and out of the memory cell. The computations of the gates of LSTM can be formulated as follow:

$$I_t = \sigma(X_t \cdot W_{xi} + H_{t-1} \cdot W_{hi} + b_i) \quad (6)$$

$$F_t = \sigma\left(X_t \cdot W_{xf} + H_{t-1} \cdot W_{hf} + b_f\right) \quad (7)$$

$$O_t = \sigma(X_t \cdot W_{xo} + H_{t-1} \cdot W_{ho} + b_o) \quad (8)$$

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

$$\tilde{C}_t = tanh(X_t \cdot W_{xc} + H_{t-1} \cdot W_{hc} + b_c) \quad (9)$$

$$C_t = F_t \odot C_{t-1} + I_t \odot \tilde{C}_t \quad (10)$$

$$H_t = O_t \odot tanh(C_t) \quad (11)$$

The output of both convolutional as well as LSTM paths are concatenated and passed to the FFN module as follows:

$$\boldsymbol{c = Concat\{u, v\}} \quad (12)$$

$$h_1' = FC_1(c) \quad (13)$$

$$h_2' = FC_2(h_1') \quad (14)$$

Following, the SoftMax layer is introduced for mapping the non-normalized vectors from FNN to a probability distribution of estimate classes:

$$\tilde{y}_c = SoftMax(h_2') = \frac{exp(h_2')}{\sum_1^c exp(h_2')} \quad (15)$$

Given that convolutional LSTM was designed to perform classification for three or more class of data in IIoT, the categorical cross-entropy function is applied as objective as follow:

$$loss = -\sum_{c=1}^{C} y_c \, log \, (\tilde{y}_c) \quad (16)$$

whereby y_c is the actual class and $\tilde{y}_c$ is the model calculated class. each industrial actor individually trains the suggested convolutional LSTM using their individual dataset. Every industrial agent first changes model parameters depending on the provided updated parameter estimation in the $r - th$ communications process with the server.

3.4. Federated Pipeline

Using a created federated learning framework and a fully encrypted messaging mechanism, the primary idea behind the FED-SEC method is to link together various IIoT users to create a deep-learning cyber-attack detection model. The FED-SEC procedure can be broken down into five distinct steps, which are outlined below (for an overview of these steps, see Algorithm 2).

Step 1: A secured connection between the cloud server and each industrialized device is set up during the installation phase of the system, during which the trust agency, leads to good the entire system by producing the public key and the secret key utilized in the fully encrypted messaging system. Next, the server decides on a set of training variables for the convolutional LSTM, including the learning rate, exponentially decaying rates for moment estimations, a tiny factor used for mathematical stabilization, the loss function, and the batch size. In addition, each industrial device informs the cloud server about the size of its personal data resource, and the cloud server then calculates a participation proportion for each industrial device. Finally, let's construct a positive integer R to represent the total iterations of cloud server-to-industrial client interaction.

Step 2: Every industrial client obtains the initial model parameters from a cloud server, and then trains a convolutional LSTM locally using its own personal data repository. Algorithm 1 provides a concise overview of the entire training process. It is anticipated that sufficient computational capacities could be given, as the local model training is done offline, whilst the computational cost of this technique is not a major concern.

Step 3: The parameters of a locally convolutional LSTM are encrypted during training by each industrial actor. Afterward, each industrial device uploads the encryption parameters of its local convolutional LSTM to a remote server.

Step 4: The cloud server compiles all of the information, including the participation percentages and protected model parameters from all of the operational actors. After that, the accumulated ciphertexts are delivered to the different industrial partners.

Step 5: Deciphering the ciphertexts allows each industrial entity to acquire the most recent version of the model's updates. The updates of the local convolutional LSTM are then adjusted after this step is completed.

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

A complete convolutional LSTM can be obtained after R cycles (an experimentally chosen criterion) of communications between the server side and client side. It is worth mentioning that during each transmission cycle, each industrial actor must perform parameter encryption and decryption duties, which in turn demand involution procedures in matrix multiply processes (which may be small). Each industrial agent's processing cost in this scenario is almost directly related to the overall number of parameters in a convolutional LSTM. When averaging the model parameters of every industrial actor in a given communication cycle, the cloud server needs just multiply the times involved by the number of agents.

4. Experimental Design

The primary purpose of this section is to present the methodology that will be used to evaluate the proposed framework. This methodology will be presented in terms of experiments, a set of data descriptions, and evaluation metrics, each of which will be discussed in the subsequent subsections, respectively.

4.1. Data Description

In this study, the detection operation of the suggested framework is gauged while it is subjected to traffic coming from external IIoT networks. Specifically, the proposed system is assessed for its capability to recognize cyber-attacks in heterogeneous networks by making use of the TON IoT dataset [14]. It includes labeled network data gathered from various sources of information relating to nine types of IoT traffic: PWA, scanning, DoS, injection attacks, DDoS, normal, XSS, ransomware, backdoors, and MITM attacks. The data includes about 22 million log items, and 46 attributes, originating from 9 different devices. This study makes use of a representative sample of these data, as described in Table I below. The samples are split into two subgroups, with 80 percent designated for training and 20 percent designated for testing. In order to strike a healthy balance in the class, the MITM examples serve as oversamples of prior training.

Table 1: Class Distribution of the Ton_Iot Dataset

Class	Train	Test	Total
Backdoor	16,000	64000	80,000
denial of service (DoS)	16,000	64000	80,000
Injection	16,000	64000	80,000
man-in-the-middle	210	840	1050
Normal	20,000	80000	100,000
password cracking attacks (PWA)	16,000	64000	80,000
Ransomware	16,000	64000	80,000
Scanning	16,000	64000	80,000
cross-site scripting (XSS)	16,000	64000	80,000

4.2. Preprocessing

In order to make use of the two datasets, the samples must be sanitized by removing duplicates and null values, and then the data pieces must be standardized using min-max normalization. The training data is then subdivided into uniform subsets and distributed to the various participants in the industrial sector so that their respective local models can be trained.

4.3. Performance Metrics

The present investigation makes use of the four standard evaluation criteria in order to conduct performance analysis for the proposed framework.

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

Accuracy: This indicator fields an average value that represents the proportion of IIoT data points that have been correctly identified, and it calculates as follows:

$$Accuracy\ (A) = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \qquad (17)$$

Precision (P): It's a percentage that indicates how many potential threats are actually classified as such.

$$Precision\ (P) = \frac{TP}{TP + FP} \times 100, \qquad (18)$$

Recall (R): It's a ratio that indicates how many attempted invasions were successfully identified as such. it calculates as follows:

$$Recall\ (R) = \frac{TP}{TP + FN} \times 100, \qquad (19)$$

F1-score (F1): a metric that represents a weighted average of Precision and Recall, with the best value at 1 and the worst result at 0, and whose range is [0,1]. it calculates as follows:

$$F1 - score\ (F1) = 2 * \frac{P * R}{P + R}, \qquad (20)$$

Where FN stands for false negative, FP for false positive, TP for true positive, and TN for true negative.

4.4. Simulation Settings

The simulation tests are carried out on an HP computer that is run with a Ubuntu 64-bit operating system. The computer system is also armed with a central processing unit of type Intel (R) Xeon (R) CPU E5-2860 0@ 3.20GHz, a GPU of type NVIDIA GeForce, and RAM of type 64GB. Scientific python [15] library is utilized in order to put these FL strategies into action. 25 edge nodes are created using virtualized laptops with the same parameters, each of which has an Intel(R) Xeon(R) E5-2670 0 2.6GHz CPU and 4GB of memory. The proposed framework is trained for a total of 50 epochs using an Adamw optimization algorithm, with an initial learning rate of 0.001; the mini-batch size is assigned to 256; and the interaction intervals are set to 60.

5. Results And Discussions

In this section, we will start debating the results that were obtained from the various extensive simulations that were performed in order to formulate an interpretation that is both clear and instructive of the proposed framework.

5.1. Numerical Results

To provide evidence that the suggested scheme is effective, fair empirical comparisons are run between FED-SEC and the latest competing FL methods for detecting cyber-attacks. Table III displays the findings obtained from conducting these comparative experimentations utilizing the ToN IoT dataset. It is important to take into consideration that the FL [16] has the lowest percentage, coming in at 91.87%. Additionally, it is important to note that the proposed framework was capable of achieving considerable improvement. This achievement could be explained by the network's capacity to model the spatial-temporal representations that are present abundantly in data pertaining to IIoT traffic. In addition, the capacity of Homomorphic Encryption to circumvent malicious or low-quality parameters enables the cyber-attack detection system to be more effective and trustworthy in comparison to its cloud-based analogs.

Table 2: Performance Comparison between the Proposed Framework and the Competing Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score
DeepFed [17]	87.50±2.92	91.84±7.98	88.00±9.01	89.88±8.46
FL [16]	88.84±0.02	90.27±3.07	88.83±2.13	89.54 ±2.52
FDL [18]	89.73±0.38	89.38±6.53	87.43±4.18	88.39 ±5.10

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

FL [19]	88.58±1.46	90.79±2.56	85.73±5.08	88.19 ±3.40
Proposed	93.04±0.99	92.96±5.97	90.55±4.31	91.74±5.01

As an essential component of any federated ID system, the amount of time required for training and testing of the proposed framework is evaluated in relation to that of its rival methodologies. On both datasets, the suggested scheme displays good, but not optimal, levels of training time (see Figure 1). This is observable. This could be rationalized because the classifier is light. The encryption, decryption procedure, key distribution, and general agreement procedure all contribute to the time-consuming nature of the suggested framework.

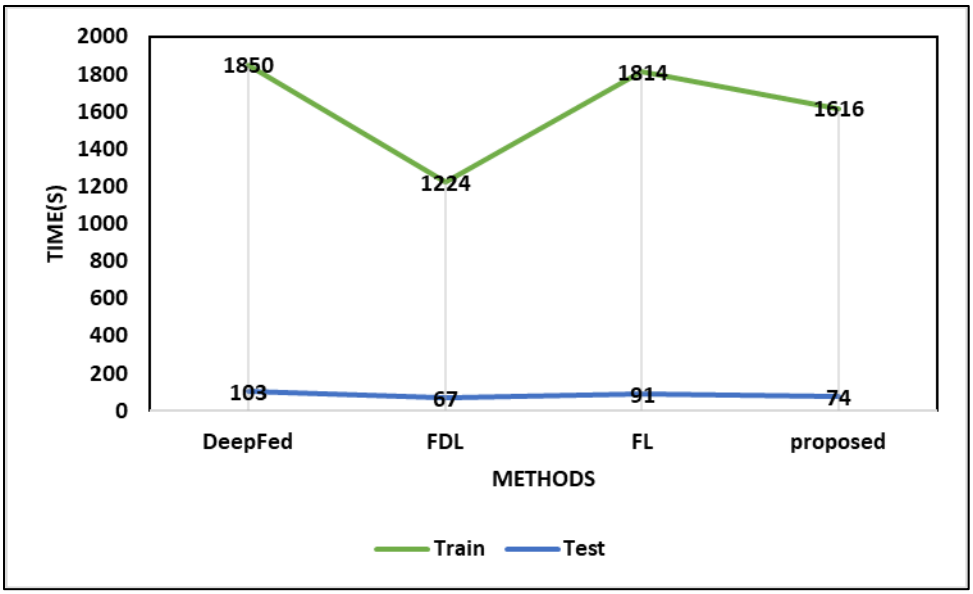

Figure 1: Comparison of the training time of different competing methods for cyber-attack detection

5.2. Statistical Analysis

A paired t-test experimentation was carried out with the statsmodels library, and the p-values that corresponded to each dataset are disclosed in Table x. Based on this test, it was determined that the results had a statistically significant impact, as stated previously. Further, over this, the significance of these results was determined to be statistically significant. The fact that the p-values are less than 0.05 demonstrates that the outcomes of using the suggested framework are statistically distinct from the outcomes of using the alternative method. This lends additional support to the findings that were drawn about the effectiveness of the proposed framework based on the comparative study that was done.

Table 3: The Statistical Findings Obtained From Paired T-Test (P-Values)

Model	Accuracy (%)	F1-score
DeepFed [17]	4.17E-04	7.00E-05
Proposed vs FL [16]	2.09E-03	3.44E-04
Proposed vs FDL [18]	9.49E-02	1.40E-04
Proposed vs FL [19]	4.72E-03	9.49E-05

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

5.3. Training schema

In addition to the experiments that were described above, additional tests are carried out in order to evaluate the effectiveness of the proposed framework in a variety of different training setups. In the beginning, the proposed framework is trained locally on the edge node utilizing only some of the available data assets. Second, the proposed framework is educated in a cooperative manner through the use of federated learning, as suggested in the proposed framework. Thirdly, it utilizes all of the data resources that are available on the cloud server in order to train itself centrally. The present findings are presented in Table VI for each assault according to their exactness and their F1-score for the ToN IoT dataset. Due to the constraints on storage space and computing power, it was obvious that the locally trained FED-SEC would result in the worst performance throughout all metrics. It is important to note that the proposed framework demonstrates efficiency overall measures in recognizing various kinds of cyber-attacks directed at edge IIoT networks. This achievement is very much on par with the outcomes that can be attained through centralized training of the proposed framework using the cloud. This provides a further explanation as to why the proposed framework is superior in terms of preserving the security and privacy of IIoT without affecting the effectiveness of the cyber-attack recognition system.

Table 4: The Class-Level Performance of the Proposed Framework under Different Training Schemes.

	Local		**federated**		**Centralized**	
Attacks	**Accuracy (%)**	**F1-score**	**Accuracy (%)**	**F1-score**	**Accuracy (%)**	**F1-score**
Backdoor	83.88±5.00	87.78±2.87	89.68±1.22	89.29±0.95	94.11±0.89	98.12±1.94
DoS	83.04±6.30	87.15±4.50	97.06±5.25	86.03±1.04	96.40±5.49	91.57±8.20
Injection	83.98±0.17	80.08±0.34	90.84±8.84	81.80±8.16	88.50±0.15	87.64±1.98
MITM	81.87±3.24	79.76±6.62	94.93±8.60	95.20±1.21	97.83±3.57	98.62±3.93
Normal	83.93±2.98	87.81±6.23	93.03±1.56	94.81±5.00	95.03±4.76	92.62±5.09
Password	85.52±3.61	85.48±2.52	90.33±6.67	86.07±3.85	91.80±6.91	91.65±8.23
Ransomware	81.71±5.36	80.20±7.13	91.05±7.12	95.25±2.18	98.26±4.69	98.64±5.36
Scanning	80.45±4.57	81.09±1.68	96.16±5.47	96.33±1.94	97.14±3.96	98.36±6.26
XSS	73.50±8.69	72.27±5.34	86.10±8.05	86.92±0.51	89.47±2.87	89.30±2.88

6. Conclusions And Future Work

In order to identify and mitigate cyberattacks on IIoT, we present a federated deep learning method here called FED-SEC. To begin, we created a novel federated learning architecture for numerous IIoT, which enables the collaborative construction of a comprehensive cyberattack detection model without compromising individual privacy. We have developed a novel cyberattack detection model based on a convolutional neural network and a genetic relational algorithm, which is capable of effectively detecting a wide range of cyberattacks aimed at IIoT. Model parameters are kept secure and private throughout training with the help of a fully secure communication protocol developed for the FED-SEC. Comprehensive trials on a genuine IIoT dataset show that the suggested FED-SEC strategy is both more effective and superior to state-of-the-art techniques. The suggested system primarily constructs a federated cyberattacks detection model for same-domain IIoT, which is an important consideration.

References

[1] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022

in Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2020.3023430.

[2] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward Effective Intrusion Detection Using Log-Cosh Conditional Variational Autoencoder," *IEEE Internet Things J.*, 2021, doi: 10.1109/JIOT.2020.3034621.

[3] N. Ravi and S. Mercy Shalinie, "Semisupervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.2993410.

[4] G. Muhammad, M. S. Hossain, and S. Garg, "Stacked Autoencoder-based Intrusion Detection System to Combat Financial Fraudulent," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.3041184.

[5] R. Zhao *et al.*, "A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3119055.

[6] H. Grover, T. Alladi, V. Chamola, D. Singh, and K. K. R. Choo, "Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles," *IEEE Internet Things J.*, 2021, doi: 10.1109/JIOT.2021.3071362.

[7] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.2970501.

[8] A. Mourad, H. Tout, O. A. Wahab, H. Otrok, and T. Dbouk, "Ad Hoc Vehicular Fog Enabling Cooperative Low-Latency Intrusion Detection," *IEEE Internet Things J.*, 2021, doi: 10.1109/JIOT.2020.3008488.

[9] F. Khan, M. A. Jan, A. U. Rehman, S. Mastorakis, M. Alazab, and P. Watters, "A Secured and Intelligent Communication Scheme for IIoT-enabled Pervasive Edge Computing," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2020.3037872.

[10] 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.*, 2022, doi: 10.1109/JIOT.2021.3077803.

[11] 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.*, 2022, doi: 10.1109/JIOT.2021.3100755.

[12] B. Hou *et al.*, "Mitigating the Backdoor Attack by Federated Filters for Industrial IoT Applications," *IEEE Trans. Ind. Informatics*, 2022, doi: 10.1109/TII.2021.3112100.

[13] P. Ruzafa-Alcazar *et al.*, "Intrusion Detection based on Privacy-preserving Federated Learning for the Industrial IoT," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2021.3126728.

[14] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, 2020, doi: 10.1109/access.2020.3022862.

[15] T. Ryffel *et al.*, "A generic framework for privacy preserving deep learning," Nov. 2018, [Online]. Available: http://arxiv.org/abs/1811.04017.

[16] Y. Liu *et al.*, "Deep Anomaly Detection for Time-series Data in Industrial IoT: A Communication-Efficient On-device Federated Learning Approach," *arXiv*, vol. 4662, no. i, pp. 1–11, 2020, doi: 10.1109/jiot.2020.3011726.

[17] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, pp. 1–1, 2020, doi: 10.1109/tii.2020.3023430.

[18] 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.*, 2021, doi: 10.1109/JIOT.2021.3100755.

[19] 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.*, 2021, doi: 10.1109/JIOT.2021.3077803.

Doi: https://doi.org/10.54216/JISIoT.070105
Received: March 28, 2022 Accepted: October 26, 2022