Securing IoT Environment by Deploying Federated Deep Learning Models

Saleh Alghamdi, Aiiad Albeshri
Faculty of Computer Sciences, King Abdulaziz University, Jeddah, Saudi Arabia

***Abstract*—The vast network of interconnected devices, known as the Internet of Things (IoT), produces significant volumes of data and is vulnerable to security threats. The proliferation of IoT protocols has resulted in numerous zero-day attacks, which traditional machine learning systems struggle to detect due to IoT networks' complexity and the sheer volume of these attacks. This situation highlights the urgent need for developing more advanced and effective attack detection methods to address the growing security challenges in IoT environments. In this research, we propose an attack detection mechanism based on deep learning for federated learning in IoT. Specifically, we aim to detect and prevent malicious attacks in the form of model poisoning and Byzantine attacks that can compromise the accuracy and integrity of the trained model. The objective is to compare the performance of a distributed attack detection system using a DL model against a centralized detection system that uses shallow machine learning models. The proposed approach uses a distributed attack detection system that consists of multiple nodes, each with its own DL model for detecting attacks. The DL model is trained using a large dataset of network traffic to learn high-level features that can distinguish between normal and malicious traffic. The distributed system allows for efficient and scalable detection of attacks in a federated learning network within the IoT. The experiments show that the distributed attack detection system using DL outperforms centralized detection systems that use shallow machine learning models. The proposed approach has the potential to improve the security of the IoT by detecting attacks more effectively than traditional machine learning systems. However, there are limitations to the approach, such as the need for a large dataset for training the DL model and the computational resources required for the distributed system.**

***Keywords*—Internet of Things (IoT); security breaches; machine learning; Deep Learning (DL)**

I. Introduction

IoT security has attracted more attention as a result of the Internet of Things (IoT) technologies' quick growth and wide use. IoT is a network system comprising numerous IoT devices that can be accessible to cyber-attacks because they are typically found in unsupervised locations. One of the most difficult study areas in information technology is cyber security. It is especially challenging to do when new technologies are involved, such as the IoT, because of its common use in numerous technological fields, the internet of things is predicted to reach 50 billion devices by the year 2020 [1]. The privacy, integrity, and availability of data are seriously threatened by this growth, which malevolent actors may use against them. In addition to preventing illegal access to networks and systems, cyber security also involves protecting data and personal information. As more and more new applications depending on connected devices are created, there has been an increased focus on IoT security in recent years. In comparison to computer networks, attacks on the Internet of Things could make things worse and result in significant, extremely expensive damage. IoT is so strongly dependent on the reduction of end security setup, and all IoT strategies and components should completely address security threats. In light of research into IoT risk categories and security architecture, the detection methods need to be improved [2].

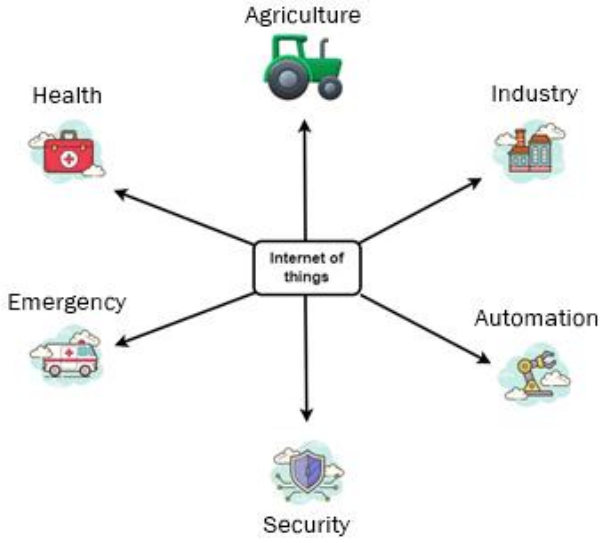

Fig. 1. Internet of things.

Attacks on linked devices have become a serious issue as IoT has gained popularity as shown in Fig. 1. IoT devices are sensitive to a variety of attacks, including denial of service, monitoring of communications, and password cracking. As the number and variety of Internet of Things (IoT) devices continue to grow, safeguarding these devices against cyber-attacks is becoming increasingly critical. Study [3-6] highlight the growing concern for the security of IoT devices, underscoring the urgency of implementing effective protective measures. Moreover, the complex nature of these interconnected systems, which often depend on wireless networks for the transmission of real-time, sensitive data, further elevates the risk of cyber threats. Such vulnerabilities can be exploited through attacks like web insertion, potentially resulting in the unauthorized access and exposure of private data, as well as the alteration or tampering of critical information. This exposure not only compromises the privacy of individuals and organizations but also threatens the integrity

and reliability of the system as a whole [7]. For IoT devices, improved, more reliable intrusion detection systems are required. For threat detection, deep learning-based security systems do not require a network connection and work with all types of devices, operating systems, and data [8].

Attack detection methods include anomaly-based and signature-based methods. The signature-based method analyzes the incoming traffic to the database's list of known attack types, whereas the anomaly-based method detects attacks as behavioural anomalies from normal traffic. The earlier method has received criticism for not being able to detect fresh attacks despite having high detection accuracy and a low false alarm rate. On the other hand, anomaly detection does not have high accuracy, but it does detect new attacks. Classical machine learning has been heavily employed in both strategies [9]. Traditional machine learning algorithms are unable to identify advanced cyber-attacks due to the attackers' continuous increase in strength and resources. The majority of these attacks are minor variations of cyber-attacks that have been seen before. It is noticeable that even the as such unique attacks (1% of all attacks) depend on earlier concepts and logic [10-11].

Unlike traditional machine learning methods that struggle with abstract feature extraction, DL can develop high-level, stable representations of training data, making it sensitive to slight variations or modifications. This sensitivity is particularly useful in fields like pattern recognition, computer vision, and image processing, where DL has significantly improved classification and prediction accuracy. The passage highlights recent findings that suggest DL's effectiveness in traffic classification and intrusion detection systems, indicating its novel application in cyber security attack detection, even within resource-constrained networks. The research aims to develop a distributed attack detection mechanism based on DL for the IoT, leveraging DL's self-learning capability to enhance accuracy and processing speed.

This research makes the following contributions:

- Develop and deploy an attack detection mechanism based on federated learning and deep learning that captures the distribution patterns of IoT networks.
- The proposed system can identify attacks as soon as they occur and respond swiftly to mitigate future damage.
- The proposed system can reduce the probability of false positives by learning and adapting to new attack patterns.

The Section II provides a background study; Section III outlines the proposed methodology, followed by the results in Section IV. Finally, the paper is concluded in Section V.

II. Literature Review

Many researchers have used different techniques on different types of data for user behaviour. Each researcher explores different aspects of user behaviour analysis. Here the study discusses a few of them, especially for Anomaly Detection in the Internet of Things.

In study [14], author discusses the rapid growth of the Internet of Things (IoT) industry, projected to reach 30.9 billion devices by 2025, and the associated security risks due to manufacturers prioritizing service quality over security. In response to the significant challenge posed by detecting intrusions within the extensive and diverse networks of the Internet of Things (IoT), the authors propose a sophisticated solution. They have developed an intrusion detection system that utilizes the capabilities of deep learning to effectively address this issue. This system is uniquely designed to be highly adaptable, enabling it to learn from and adjust to the intricacies of any IoT network it encounters. One of the most notable achievements of this system is its exceptional accuracy rate, which stands at 93.74%. This level of precision underscores the system's effectiveness in identifying and responding to security breaches across the varied landscape of IoT environments. In study [15], the authors address the security vulnerabilities of the Industrial Internet of Things (IIoT) to protect against sophisticated multi-variant botnet attacks. This approach utilizes a combination of supervised and unsupervised machine learning algorithms to develop an Intrusion Detection System (IDS) that outperforms existing methods in speed and accuracy of bot attack detection, showcasing its effectiveness through comprehensive evaluations using the latest datasets and performance metrics. In study [16], the paper explores the implementation of machine learning-based Intrusion Detection Systems (IDS) in IoT environments with limited resources. The proposed IDS combines Principal Component Analysis (PCA) for feature reduction with various machine learning models, achieving high detection accuracy against contemporary attacks as demonstrated using the UNSW-NB15 datasets. The approach prioritizes reducing communication overhead and avoiding the complexities of encryption methods, with future work aimed at enhancing this model with deep learning techniques and novel datasets for broader IoT applications.

In this study, [17] researchers tackle the challenge of safeguarding Industrial Internet of Things (IIoT) edge devices from cyber-threats and anomalies to enhance threat detection. Their method demonstrates a high accuracy of 99.5% on an IIoT-specific dataset, surpassing traditional ML-based classifiers in metrics like precision, F1-score, and recall. In [19], a novel intrusion detection architecture named DRaNN is introduced for improving security in IIoT settings, employing a hybrid approach of particle swarm optimization (PSO) and sequential quadratic programming (SQP) for optimizing hyperparameters for enhanced attack detection. The study in [20] explores a DL-based method for bolstering blockchain data security, focusing on the identification and deployment of secure smart contracts within public blockchain networks. This approach achieves notable results in vulnerability detection accuracy (99.083%), precision (91.935%), and recall (87.692%).

TABLE I. LITERATURE REVIEW

Paper Title	Dataset	Methodology	Domain	Limitations
[23]	KDD Cup 1999 datasets	deep neural network	IoT security	Benchmark dataset not used
[24]	UNSW-NB15 datasets	CNN+RNN	IoT security	The system may not be effective against attacks that do not generate anomalous traffic patterns
[25]	CICIDS2017 dataset	BiLSTM	IoT security	Low performance in some type of attacks
[26]	Various IoT datasets	CNN	IoT security	Small datasets
[27]	UNSW-NB15 dataset	RNN+Blockchain	IoT security	The proposed approach may not be effective against attacks that do not generate anomalous network traffic patterns.

In study [21], researchers propose a unique pairing structure and algorithm to verify the authenticity of sensor data within the IoT framework. Their method is validated through case studies and experiments on two real-world datasets, applying CART, SVM, and KNN algorithms. Lastly, [22] presents an innovative architecture designed to detect and counteract DoS/DDoS attacks in IoT environments, offering precise detection capabilities that identify both the attack type and the packet type involved. Some studies are detailed in Table I, showcasing advancements in IoT security through various approaches.

III. PROPOSED MODEL

The proposed system used a Federated Learning (FL) approach to overcome the challenges of anomaly detection in the Industrial Internet of Things (IIoT) ecosystem, where devices often have limited capabilities and generate minimal data. This method involves aggregating training data from multiple users to quickly develop a robust model, with local FL clients training models on available data and a global server aggregating these insights to improve both global and local models. This strategy enhances the ability to differentiate between malicious and benign traffic within an IIoT network. In Fig. 2, the configuration of the proposed FL approach for IIoT intrusion detection is depicted, with several installed and network-connected devices spread across various places [28].

A. Learnings and Intelligence at the Local Level

In this component of the framework, each client (ranging from k=1 to K) locally trains the data collected from their respective Industrial Internet of Things (IIoT) devices using the models provided by the server. Concurrently, an Intrusion Detection System (IDS) at the client's site identifies any potential attacks. Additionally, a network data analyzer is employed to log data for subsequent analysis. This approach of enabling local training, adjusting parameters, and refining the inference mechanisms, ensures the autonomy of local intrusion detection systems through intelligent, device-level learning.

B. Distribution of Learnings

To enhance the intrusion detection system by optimizing its parameters, clients share their individually trained models with a centralized server for aggregation. This process of model exchange is managed by an intelligent communication administrator, such as a security gateway. This collaborative approach aims to refine and improve the system's ability to detect intrusions effectively.

C. Model and Assumptions

In an Industrial Internet of Things (IIoT) network, a threat or adversary, referred to as M, can originate from either inside or outside the network. This includes insiders, such as compromised IIoT devices or other connected devices that remain within the network's confines, as well as external attackers who exploit the Internet to conduct cyberattacks. These attacks may involve manipulating digitally connected systems, inserting harmful content into databases, or pilfering sensitive information. IIoT malware often seeks out devices with lax security measures to serve as a foothold for launching attacks, aiming to identify and exploit weaknesses in IIoT systems and devices. We also made a few more assumptions during our analysis. These are what they are:

- A reliable FL aggregator is vital because aggregation servers play a crucial role in the learning process. For this reason, there must always be some level of faith in the system that organizes learning.
- No nefarious IIoT Device by Design: In some circumstances, newly introduced IIoT products may already have security issues. However, before being used for their intended function, these gadgets must not be contaminated or diseased.
- Secure Clients: Assuming that secure clients are essential for Federated Learning (FL) in IIoT systems, we proceed under the presumption that they exist.

D. Intrusion Detection for FL

In the Federated Learning (FL) model, each of the K clients independently trains a local model based on a common global model distributed by the server, utilizing their unique local datasets instead of relying on a centralized data repository. These clients then securely transmit the insights gained from local training sessions to an aggregation server via an SSL/TLS secured connection. The aggregation server merges these individual contributions to update the global model, optimizing it with the best possible parameters. This process is iterated through several rounds of federated learning, denoted by R, starting from initial weights represented by w, until the model converges to an optimal state. The model weights update during each communication round is guided by a formula derived from the FedAvg algorithm, ensuring efficient and effective learning from each local client's data.

$$w_{t+1} = \sum_{k+1}^{k} \frac{n_k}{n} w_{t+1}^{k} \quad (1)$$

In this context, n_k represents the dataset size for each individual client, while n signifies the total dataset size across all clients. After the iteration process, the updated global model is denoted as w_{t+1}^k. Fig. 3 illustrates the connections between various participants in the Federated Learning (FL) IIoT intrusion detection system. For inclusion in the FL cycle, the server selects clients that are connected to operational IIoT devices, which must be turned on, plugged into a power source, and linked to an unmetered Wi-Fi connection. The interaction among the system's components to facilitate the FL process is outlined as follows:

1) The server initializes a NN model based on a global intrusion detection framework, specifying parameters such as the number of neurons, epochs, and hidden layers. The initial weights of this model are symbolized by w.

2) Clients maintain the confidentiality of their local data while leveraging it to refine the model using information from the IIoT devices they manage.

3) To safeguard client privacy, only the parameters of the updated model, which contribute to the enhanced intrusion detection capabilities, are shared with the central server.

4) Upon collecting all the updates, the server aggregates the weights from each client's model to form an updated, improved global model using the FedAvg algorithm. This aggregation takes into account the dataset size at each client node.

5) The central server pushes the modified model parameters back to the clients.

6) Every client applies the updated model parameters and modifies them in light of the fresh information.

7) Repeat steps 4, 5, 6, and 7 to continue refining and improving the model.

E. Machine Learning Classifiers for Intrusion Detection

The rapid development of ML methods and applications has given the intelligent IDS solution an altogether novel avenue for development. To extract better data representations for powerful model construction, neural network methods have proven to be highly helpful. Neurons, weights, biases, and functions are the essential elements that all neural networks share, even though there are many different types of neural networks. For intrusion detection, we have maintained a minimal number of classifiers at a central location, utilizing the following two:

CNNs are designed to process data represented in multiple arrays. At the core of this approach are the initial layers, which consist of a set of learnable filters applied via convolutional feature extractors. These filters are employed across the input data using a sliding window mechanism. The term "stride" denoting the extent of overlap between these filters' applications. Convolutional kernels, essential elements of a CNN layer, are utilized to create unique feature maps by connecting neurons to local regions in the preceding layer's feature map. To form a feature map, the kernel is systematically applied across all spatial positions of the input. After constructing convolutional and pooling layers, classification is achieved through one or more densely connected layers.

$$h_j^{(n)} = \sum_{k=1}^{k} h_k^{(\cap-1)} * w_{k_j}^{(n)} + b_{k_j}^{(n)} \qquad (2)$$

Recurrent Neural Networks (RNNs) are advanced models of feed-forward neural networks, designed to retain information at each stage for future outputs. In an RNN, the output from neurons is fed not only to their own input but also to the input of other neurons. This design allows RNNs to process sequences of data and time series effectively by leveraging their internal memory.

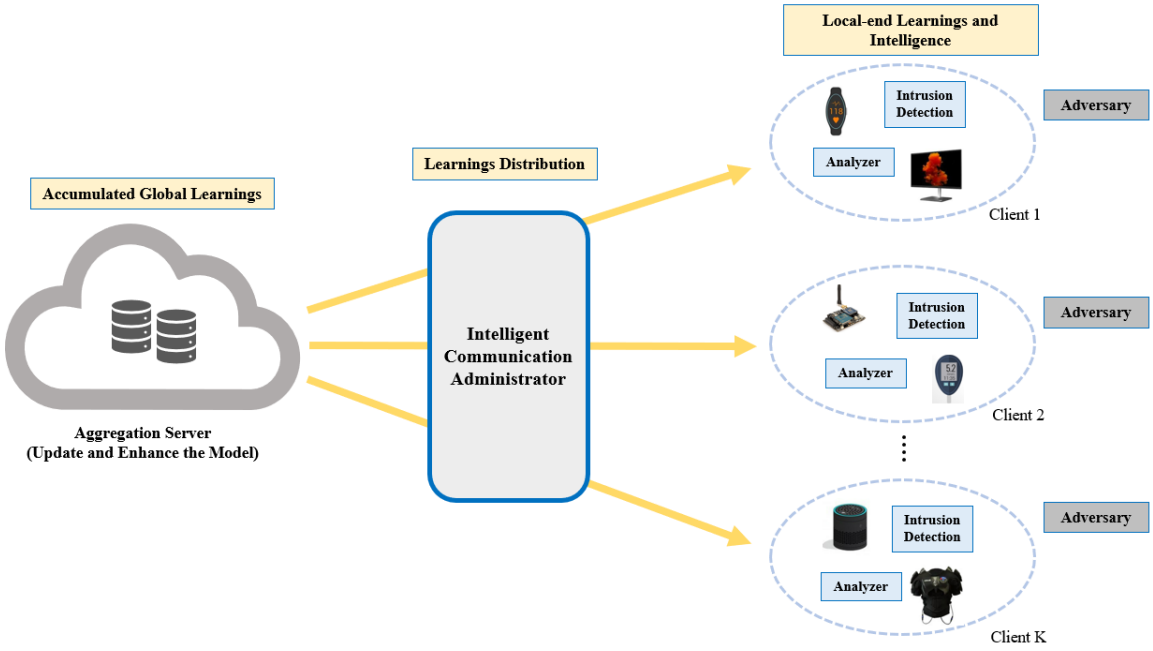

Fig. 2. Proposed approach.

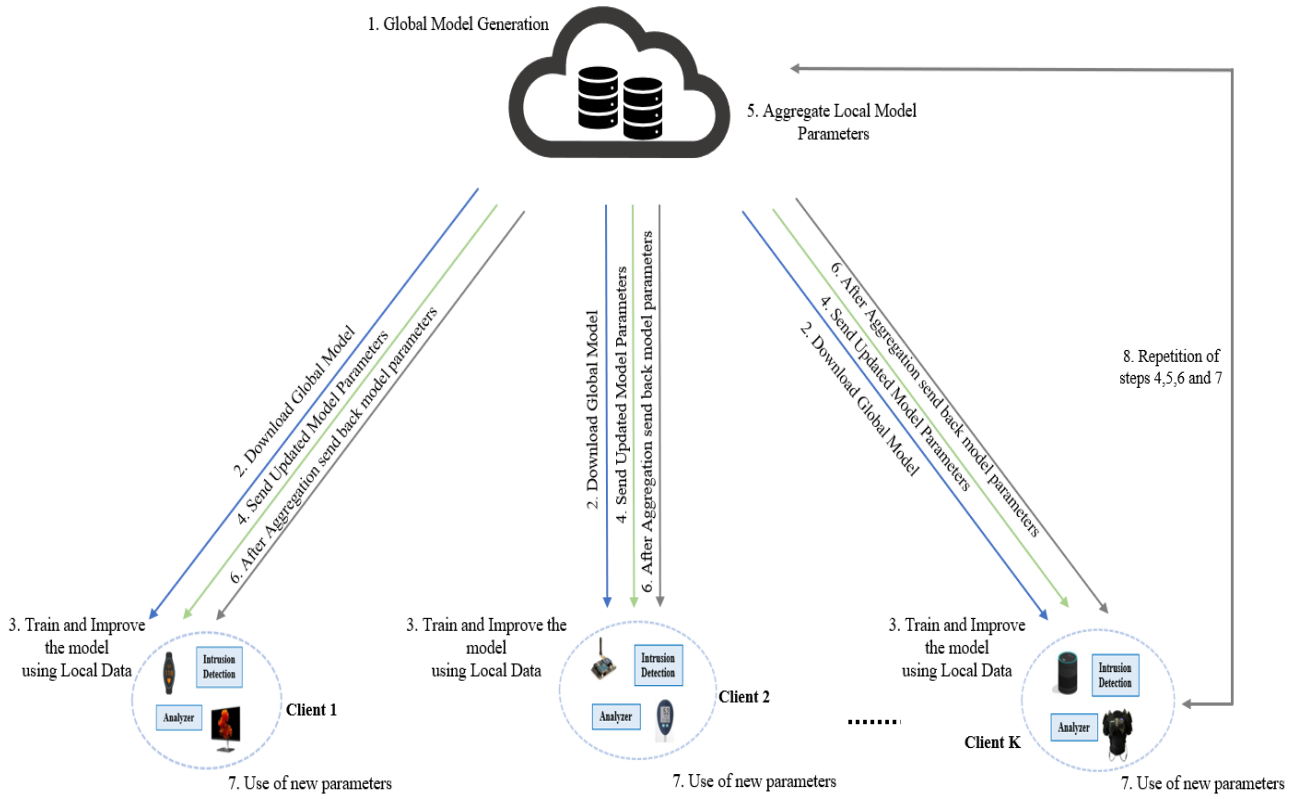

Fig. 3. Interactions among FL-based IDS clients' participants.

VI. Experimental Results

For training and evaluating Intrusion Detection Systems (IDSs) in IIoT networks, selecting an appropriate dataset is crucial. To address this need in IIoT and IoT contexts, a novel cybersecurity dataset named Edge-IIoTset has been introduced. The dataset includes data from a wide range of IoT devices, including heart rate monitors, flame detectors, and sensors for temperature and humidity. For Federated Learning (FL) projects, it's crucial that the dataset showcases a distribution that is both imbalanced and non-independently and identically distributed (Non-IID), reflecting the complexity of real-world situations accurately. Our dataset (Edge-IIoTset) has been partitioned for experimental purposes into several local datasets so that they can be trained to meet FL's requirements. Due to the lack of FL-specific datasets, this was necessary. The dataset breakdown is shown in Table II.

TABLE II. Training and Testing Distributed Data

Dataset	Total	Training	Testing
Normal	25,320	21,112	5933
DDoS-UDP Attack	15498	12540	3033
DDoS-ICMP Attack	13090	10179	2899
Uploading Attacks	10,147	8261	2017
DDoS-TCP Attack	10,380	9045	2302

To assess the effectiveness of FL, we ran several tests with 3 to 15 clients contributing to model training. Before achieving the best results, our model was trained for a total of 50 epochs. While creating the federated model, we looked at how effective the system was for various client counts. The deployment dataset's training data was distributed to each client, a random selection from which was made. We created three federated models and compared them to a centralised model to investigate this potential loss in accuracy. The training dataset was distributed among 3, 9, and 15 clients.

A. Performance Metrics

When evaluating the model using test data, the following performance metrics were considered:

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Pre = \frac{TP}{TP+FP} \quad (4)$$

$$Rec = \frac{TP}{TP+FN} \quad (5)$$

$$F1 = 2 . \frac{Precision.Recall}{Precision+Recall} \quad (6)$$

B. Evaluation of Performance

This section covers the results of the experiment employing centralised learning and the performance of our suggested FL-based model for incursion detection using the Edge IIoT set dataset.

1) Using centralised method for intrusion detection: We first employed two conventional centralised ML methods, namely CNN and RNN, to assess the performance of the new model. In the method we propose, Table III lists the values assigned to the parameters of various classifiers.

TABLE III. ML CLASSIFIER SETTINGS

Classifier	Parameters
CNN	Filters Pooling layer Hidden notes Hidden layers
RNN	Batch size Local epochs Loss function Activation function

Table IV presents the performance metrics of machine learning techniques for a centralized model, focusing on their ability to differentiate between benign and attack classes within the dataset. According to the table, both RNN and CNN methods exhibit high effectiveness, with Accuracy and F1-Score reaching up to 94% and 93%, respectively. Furthermore, these techniques demonstrate excellent capability in distinguishing between benign and malicious activities, achieving Precision and Recall rates as high as 95% for RNN and 94% for CNN.

2) Using federated method for intrusion detection: We conducted Federated Learning (FL) experiments using our model with three different sets of clients, denoted as K, where K equals 3 for the first set, 9 for the second set, and 15 for the third set. To address our varied client base, we employed two scenarios:

- Independent and Identically Distributed (IID): In this scenario, each client's data distribution is uniform across the dataset.
- Non-Independent Identically Distributed (Non-IID): In this scenario, the overall dataset's data distribution varies from that of each individual client.

C. Comparison to Related Works

Table V outlines a comparative analysis against similar methodologies encompassing various dimensions such as deployment year, datasets utilized, machine learning classifiers, number of clients, and data distribution strategies. This comparison reveals that our proposed model uniquely tackles both IID and Non-IID data issues, demonstrating effective performance across these data types as discussed in the preceding section.

D. Discussion

Utilizing Federated Learning (FL) instead of traditional Machine Learning (ML) techniques offers significant advantages for Industrial Internet of Things (IIoT) devices in terms of data security and bandwidth efficiency. By adopting FL, IIoT devices can transmit data that is not only more secure but also requires less bandwidth. This is because, in an FL setup, the vast amounts of private and sensitive information are not centralized on a single server. Instead, clients only share the outcomes of their individual local model trainings, substantially reducing bandwidth needs [13] [18]. This approach not only ensures the security of the data but also upholds the privacy of the users since the raw data remains on the device. Additionally, FL enables devices to autonomously predict and detect network anomalies, even when offline, by leveraging the local representations of the models [30]. This implies that local clients are able to persist with their model training and intrusion detection efforts, irrespective of their connectivity status. Furthermore, with an increase in the number of Federated Learning (FL) rounds, the precision of intrusion detection nears that of centralized Machine Learning (ML) models. This improvement in performance is attributed to the cumulative enhancements from client-end learnings, allowing the models to operate with the same efficacy as centralized models after each FL round.

TABLE IV. ASSESSMENT OF THE CENTRAL INTRUSION DETECTION MODEL

Class	Accuracy		Precision		Recall		F1-Score	
	CNN	**RNN**	**CNN**	**RNN**	**CNN**	**RNN**	**CNN**	**RNN**
Normal	0.94	0.95	0.93	0.91	0.91	0.91	0.92	0.91
DDoS-UDP Attack	0.89	0.90	0.95	0.96	0.89	0.88	0.90	0.91
DDoS-ICMP Attack	0.83	0.81	0.80	0.78	0.88	0.87	0.83	0.81
Uploading Attacks	0.74	0.79	0.78	0.83	0.63	0.78	0.71	0.80
DDoS-TCP Attack	0.91	0.92	0.91	0.93	0.91	0.93	0.93	0.92
Proposed model	0.94	0.96	0.93	0.92	0.93	0.95	0.94	0.95

TABLE V. COMPARSION OF PROPOSED MODEL WITH BASELINES

IoT IDS	Year	Dataset	Classifier	IID	Non-IID
Nguyen et al [27]	2020	Private Dataset	RNN-GRU	No	Yes
Li et al [28]	2021	Gas Pipeline	CNN-GRU	Yes	Yes
Huong et al [29]	2022	Bot-IoT	LocKedge	No	Yes
Proposed model	2022	Edge-IIoTSet	CNN RNN	Yes	Yes

V. CONCLUSION

This study introduces an innovative intrusion detection system that leverages federated machine learning (ML) to tackle the vital concerns of security and privacy within IoT networks. Our key goal was to identify and stop unauthorized intrusions, which would ultimately ensure the security of IoT networks. We carried out extensive experiments with a freshly created dataset called Edge-IIoTset to verify the efficacy of our strategy. These tests were conducted using two well-known ML models: CNN and RNN, on both centralised and federated systems. The experimental results showed that our suggested federated learning (FL) approach can produce competitive results in the area of intrusion detection, which was quite encouraging. Our technology demonstrated its capacity to successfully identify intrusions in IoT networks by utilizing the power of collaborative learning while protecting data privacy. We also performed a thorough comparative analysis, comparing our method to previous FL-based intrusion detection systems in independent and non-independent, identically distributed (IID and non-IID) scenarios. The studies in our research help to demonstrate the viability, applicability, and utility of our suggested approach. They greatly advance our knowledge of and ability to use federated learning in the context of IoT networks. The results of our study highlight FL's potential as a workable option for boosting the security and privacy of IoT systems.

REFERENCES

[1] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, 2021, doi: 10.1007/s11831-020-09496-0.

[2] Y. Li, Y. Zuo, H. Song, and Z. Lv, "Deep Learning in Security of Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22133–22146, 2022, doi: 10.1109/JIOT.2021.3106898.

[3] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," *Multimed. Tools Appl.*, vol. 79, no. 5–6, pp. 3993–4010, 2020, doi: 10.1007/s11042-019-7495-6.

[4] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.

[5] Q. A. Al-Haija and S. Zein-Sabatto, "An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks," *Electron.*, vol. 9, no. 12, pp. 1–26, 2020, doi: 10.3390/electronics9122152.

[6] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, 2017, doi: 10.1109/MIC.2017.37.

[7] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey BT - Wireless Algorithms, Systems, and Applications," pp. 685–695, 2015.

[8] H.-J. Nam *et al.*, "Security and Privacy Issues of Fog Computing," *J. Korean Inst. Commun. Inf. Sci.*, vol. 42, no. 1, pp. 257–267, 2017, doi: 10.7840/kics.2017.42.1.257.

[9] V. T.-2017 I. W. C. and and undefined 2017, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," *ieeexplore.ieee.org*, Accessed: Mar. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7925567/

[10] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," *APSIPA Trans. Signal Inf. Process.*, vol. 3, 2014, doi: 10.1017/ATSIP.2013.99.

[11] Guy Caspi, "Introducing Deep Learning: Boosting Cybersecurity ...", [Online]. Available: https://www.darkreading.com/analytics/introducing-deep-learning-boosting-cybersecurity-with-an-artificial-brain/a/d-id/1326824?

[12] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Int. Conf. Bio-inspired Inf. Commun. Technol.*, 2015, doi: 10.4108/eai.3-12-2015.2262516.

[13] L. Yuancheng, M. Rong, and J. Runhai, "A Hybrid Malicious Code Detection Method based on Deep Learning," *Int. J. Secur. Its Appl.*, vol. 9, no. 5, pp. 205–216, 2015.

[14] A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," *Computers*, vol. 12, no. 2, 2023, doi: 10.3390/computers12020034.

[15] T. Hasan *et al.*, "Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach," *IEEE Trans. Netw. Sci. Eng.*, 2022, doi: 10.1109/TNSE.2022.3168533.

[16] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 9395–9409, 2022, doi: 10.1016/j.aej.2022.02.063.

[17] A. Yazdinejad, B. Zolfaghari, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "Accurate threat hunting in industrial internet of things edge devices," *Digit. Commun. Networks*, 2022, doi: 10.1016/j.dcan.2022.09.010.

[18] T. A. Al-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*, vol. 22, no. 9, 2022, doi: 10.3390/s22093400.

[19] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, and N. Pitropakis, "DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8112–8121, 2022, doi: 10.1016/j.jksuci.2022.07.023.

[20] R. Gupta, M. M. Patel, A. Shukla, and S. Tanwar, "Deep learning-based malicious smart contract detection scheme for internet of things environment," *Comput. Electr. Eng.*, vol. 97, 2022, doi: 10.1016/j.compeleceng.2021.107583.

[21] U. Ahmad, "A node pairing approach to secure the Internet of Things using machine learning," *J. Comput. Sci.*, vol. 62, 2022, doi: 10.1016/j.jocs.2022.101718.

[22] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Comput. Electr. Eng.*, vol. 98, 2022, doi: 10.1016/j.compeleceng.2022.107716.

[23] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, "A Hybrid Deep Learning Model with Self-Improved Optimization Algorithm for Detection of Security Attacks in IoT Environment," Future Internet, vol. 14, no. 10, p. 301, Oct. 2022, doi: 10.3390/fi14100301.

[24] M. A. Khan et al., "A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT," Sensors, vol. 21, no. 21, p. 7016, Oct. 2021, doi: 10.3390/s21217016.

[25] S. Sriram, R. Vinayakumar, M. Alazab, and K. P. Soman, "Network flow based IoT botnet attack detection using deep learning", In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp. 189-194, 2020.

[26] Y. Song, D. Zhang, Y. Li, "Intrusion Detection for Internet of Things Networks using Attention Mechanism and BiGRU", In 2023 5th International Conference on Electronic Engineering and Informatics (EEI), pp. 227-230, 2023.

[27] S. Ali, O. Abusabha, F. Ali, M. Imran, and T. Abuhmed, "Effective Multitask Deep Learning for IoT Malware Detection and Identification Using Behavioral Traffic Analysis," IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1199–1209, Jun. 2023, doi: 10.1109/tnsm.2022.3200741.

[28] [1]Y. Liu, T. Lin, and X. Ye, "Federated recommender systems based on deep learning: The experimental comparisons of deep learning

algorithms and federated learning aggregation strategies," Expert Systems with Applications, vol. 239, p. 122440, Apr. 2024, doi: 10.1016/j.eswa.2023.122440.

[29] [1]O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. Mohamed, and H. Arshad, "State-of-the-art in artificial neural network applications: A survey," Heliyon, vol. 4, no. 11, p. e00938, Nov. 2018, doi: 10.1016/j.heliyon.2018.e00938.

[30] S. Li, W. Li, C. Cook, C. Zhu and Y. Gao, "Independently recurrent neural network (indrnn): Building a longer and deeper rnn", In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5457-5466, 2018.