FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network

Parya Haji Mirzaee*, Mohammad Shojafar*, Zahra Pooranian*
Pedram Asef†, Haitham Cruickshank*, Rahim Tafazolli*

* 5G & 6G Innovation Centre (5GIC/6GIC), University of Surrey, Guildford, United Kingdom
† University of Hertfordshire, Hatfield, United Kingdom

{p.hajimirzaee, m.shojafar, z.pooranian, h.cruickshank, r.tafazolli}@surrey.ac.uk

p.asef@herts.ac.uk

Abstract—In a critical infrastructure such as Smart Grid (SG), providing security of the system and privacy of consumers are significant challenges to be considered. The SG developers adopt Machine Learning (ML) algorithms within the Intrusion Detection System (IDS) to monitor traffic data and network performance. This visibility safeguards the SG from possible intrusions or attacks that may trigger the system. However, it requires access to residents’ consumption information which is a severe threat to their privacy. In this paper, we present a novel method to detect abnormalities on a large scale SG while preserving the privacy of users. We design a Federated IDS (FIDS) architecture using Federated Learning (FL) in a 5G environment for the SG metering network. In this way, we design Federated Deep Neural Network (FDNN) model that protects customers’ information and provides supervisory management for the whole energy distribution network. Simulation results for a real-time dataset demonstrate the reasonable improvement of the proposed FDNN model compared with the state-of-the-art algorithms. The FDNN achieves approximately 99.5% accuracy, 99.5% precision/recall, and 99.5% f1-score when comparing with classification algorithms.

Index Terms—Network Security, Smart Grid (SG), 5G, Intrusion Detection System (IDS), Federated Learning (FL), Advanced Metering Infrastructure (AMI).

I. INTRODUCTION

Smart Grid (SG) services, such as Advanced Metering Infrastructure (AMI), Demand Response (DR), and Real-Time Pricing (RTP), rely on online communication and information exchange systems integrated into the power network. The AMI, also known as the smart metering network, is a comprehensive distribution network of Smart Meters (SMs), sensors, relays, data aggregators, and concentrators [1]. AMI is one of the fundamental subsystems of SG, enabling both energy and information flow between customers and utilities.

Integrating wireless technologies into SG and the wide distribution and uncertain environment of AMI make this system susceptible to security attacks. Attacks such as Denial of Service (DoS) [2], Jamming [3], False Data Injection (FDI) [4], Eavesdropping [5], Man-In-The-Middle (MITM) [6], and message replay [7] can compromise either availability, integrity, or confidentiality of the system. The AMI system can be threatened by attackers pursuing different objectives, including energy and information theft, energy price manipulation, and system disruption.

Intercepting network traffic to detect suspicious or abnormal behaviour is what an Intrusion Detection System (IDS) does. IDS is an essential security strategy in the detection stage, which provides visibility for the system [8]. For real-time monitoring and fast fault detection, designing and implementing a customised IDS that operates well and satisfies the AMI requirements is necessary. Machine Learning (ML) based IDSs have been widely developed to safeguard the SG and improve the detection accuracy of the system [9]. However, the training phase of ML models requires training data to provide robust monitoring and effective detection. In this case, there is a trade-off between providing data for IDS modules to guarantee security for the SG components and protecting the users’ privacy. The privacy of householders in the concept of SG is a critical concern to be considered. Since the energy consumption measurement of customers can quickly reveal detailed information on their lifestyle.

Several approaches proposed for the privacy leakage problem of SG aim to anonymous the users’ identity or try to shape their detailed consumption under the mask of a battery charging/discharging scheme [10]. However, most of these models avoid privacy breaches at the cost of system efficiency and computation complexity [11]. In addition, recently, differential privacy has been proposed widely for obfuscating original data with additive noise [12]. Even though differential privacy can achieve privacy protection, it makes a trade-off between users’ privacy and model learnability [11]. It manipulates the data integrity, which results in accuracy detection degradation. When very accurate and faultless information is required for energy consumption, billing, and demand anticipation missions, differential privacy cannot be used widely in the metering system of SG. Thus, we require a distributed and secure model to tackle such issues. Federated Learning (FL) is a decentralised learning approach employed mainly to reduce the privacy tampering risks for users participating in a training process [13]–[15]. This model preserves the training data on the premises sides and provides a chain of connected ML models synchronised with a global model without breaching privacy laws.
A. Motivations of the paper

Generally, providing large scale, secure, and reliable SG and minimising privacy risk for the users is a crucial issue that deserves much more consideration. While major monitoring schemes require to access the SG data for evaluations, most customers are reluctant to provide their energy consumption information for utilities due to privacy concerns. This paper proposes a Federated IDS (FIDS) scheme to address the privacy leaking problem with SG consumers. FIDS applies Federated Deep Neural Network (FDNN) detection technique for monitoring traffic and designing an IDS to ensure both the security and privacy of metering infrastructure in SG. In FIDS, users are placed at the Home Area Network (HAN) and contribute with concentrators on the Neighbour Area Network (NAN) to build up a comprehensive detection model. FL requires a communication infrastructure between users and utilities to periodically share model updates. In this case, we propose the whole process to take place over a 5G network for its massive connectivity, reliability, and efficiency.

B. The main goal and contribution of the paper

This paper aims to design a distributed ML model that addresses the privacy leaking problem with SG consumers. The followings are the main contributions of this paper:

- We define a SG based infrastructure for the metering system of SG. Given the heterogeneous nature, large data volume, and critical role of SG, 5G can better serve AMI’s requirements.
- We present an FL based intrusion detection for the metering system. The customers act as participant side placed on HAN, and the data concentrator at NAN layer plays the server side role. This FL based detection system preserves the information privacy of customers much more than centralised IDS schemes.
- We provide a comparison between the proposed model, FDNN, and the centralised scenarios, in which the real data of customers is aggregated in a central IDS for analysis.

The rest of the paper is organised as follows. Section II summarises the related work done in the literature. Section III describes the proposed solution, including system modelling, architecture, problem formulation, and algorithm. In Section IV, the performance of the proposed method is evaluated. Finally, the study outcomes and achievements are discussed in Section V.

II. RELATED WORK

There has been an exhaustive investigation in the literature over incorporating ML-based algorithms into the IDS concept to overcome traditional IDS limitations such as high fault rate and zero-day attack detection [16]. Also, ML algorithms have been proposed for attack detection in various SG applications. The first widely used ML-based detector models in SG were supervised schemes [16], [17]. More sophisticated algorithms such as semi-supervised [18], unsupervised [19], reinforcement learning [20], and deep learning [21] have been proposed by the literature to achieve better accuracy and dynamic response times in detection approaches.

However, all the proposed solutions rely on centralised computation and detection architecture. In the centralised architecture [22], the monitoring process occurs at the data centre, where all SMs’ data are aggregated, analysed, and stored on a centralised processor. This deployment scheme cannot monitor the peer-to-peer traffic attacks between different nodes in the heart of AMI. Also, the implementation of centralised IDS requires high access to SMs measurements and users’ power consumption information. This approach not only increases the latency bottleneck but also triggers the privacy risk for consumers.

However, there have been some investigations within distributed detection systems also. In 2011, Zhang et al. proposed their Distributed IDS (DIDS) infrastructure, in which there is a network of IDS modules distributed at all levels of the system. Moreover, within [23], a distributed fog based detection system has been considered to defend against false metering attacks. Despite the decentralised architecture of this scheme, data transmission from residents’ entities toward the edge processors and privacy limitations were not considered. Within the embedded or fully distributed model, every household is instrumented with a Local IDS (L-IDS), and the entire detection process takes place in every node. Although this model protects the system in terms of privacy at a large scale, the system requires a surveillance data centre for better performance in the network to gain an orchestrated security framework for all components. Table I provides a summary of the IDS models proposed by literature and compares them in the case of proposed architecture and privacy consideration parameters.

Recently, a novel distributed learning scheme, FL, has explicitly been proposed to preserve users’ privacy integrated into a training model. In FL, all parties contribute to building a global model without sharing their row data and only by providing training parameters of distributed local models. This concept has raised great attention in the SG research as well. Liu et al. in [24] utilise FL for aggregating power traces of residents in a distributed model. This study considers two federated models for two differently scattered data types,
horizontal and vertical. In the horizontal model, the training occurs locally at each party, and the parameters are encrypted while sharing with the same central server. In the vertical framework, however, the clients are even reluctant to share training parameters. No real data or parameter is being shared in this case, and only critical results are shared in the encrypted model. Also, [25] presents an FL approach for the identification of electricity consumers’ characteristics. In particular, this work exploits privacy perseverance Principal Component Analysis (PCA) to extract features from SMs data and train an artificial neural network in a federated manner. The model is used for determining the socio-demographic characteristics of consumers.

However, none of these mentioned works investigated the potentiality of the FL concept for designing IDS in an AMI system. FL, by nature, is a reliable framework for scenarios in which data is distributed over several clients, and this data contains sensitive information of the customers. Motivated by this, we suggest FIDS, which is a federated detection system based on a Deep Neural Network (DNN) for the metering infrastructure of 5G. Every household in the proposed model is equipped with an IDS, classifying the raw data based on a DNN model. All these locally distributed classifiers operate on a federated basis with a global centre for synchronisation.

III. PROPOSED SOLUTION

In this section, first, the study focuses on the network architecture and communication specifications of the AMI system. Then, the problem model is sketched for expressing the proposed solution.

A. 5G-enabled Advanced Metering Infrastructure

Future 5G communication systems and SG pave the way for a sustainable and interconnected world. 5G aims to give rise to new business and industry applications for communication technologies, but it will also put new demands on the power system. Consequently, the energy sector should be able to satisfy these expectations. On the other side, SG needs a reliable, highly connected, fast, and secure communications infrastructure to operate effectively. Several industrial, commercial, and customer domains operate independently and remotely in the SG architecture but connect via an information network. There are several services with varying requirements for connectivity and Quality of Service (QoS) specifications. Although the controlling data and fault alarms require minimal delays and fast transformation speed, the measuring information’s accuracy and reliability are significantly greater. 5G technologies, however, meet most of these expectations. For instance, the 5G slicing network technology enhances spectrum efficiency and provides low end-to-end latency for SG delay-sensitive services. Also, 5G increasing connectivity and virtualization have improved the edge computing paradigm exponentially.

Fig. 1a illustrates the AMI system over a 5G network in which our proposed detection system FIDS is installed over them. 5G small cells consist of a neighbourhood and several customers’ premises. In addition, the 5G Core (5GC) is also logically distributed over gNodeB (gNB) stations at the edge of the network and within the vicinity of users. These stations operate as aggregators of the SMs’ information.

B. Federated Intrusion Detection System Architecture

FL is within the concept of collaborative learning [26]. This approach moves the code to the data location instead of the
data to the coding place [27]. In this scheme, training models are decentralised over participants, also referred to as clients, while the whole process is under the orchestration of a central surveillance server [28]. This model concentrates mainly on users’ privacy preservation and keeping training data by participants while sharing weights and bias coefficients at each training phase with a server. Finally, the server averages the measurements collected from all devices and tunes the whole system by constructing and publishing a global model [29].

The study proposes FIDS, a 5G federated architecture in the metering network of 5G, to preserve customers’ privacy along with building a distributed IDS architecture. Fig. 1b presents FIDS architecture. This system consists of two layers, participants’ and server’s layer or side. SMs installed at customers’ premises act the participants’ role, and the data concentrator placed on the neighbour network is rolling the server responsibilities. The participants’ layer, representing with a black rectangle on the left side in Fig. 1b, includes households, and each household is equipped with a Local IDS (i.e., L-IDS), which monitors the traffic and alarms or reports the surveillance centre in case of any anomaly detected within the local data of each customer. The dashed red square around each household indicates a home network, i.e. HAN. The blue rectangle on the right side of Fig. 1b demonstrates the server side and a concentrator installed on the neighbour network, i.e. NAN. After the local training phase, local models of each user in a lower layer are aggregated by data aggregators. The NAN server at the upper layer of Fig. 1b, after averaging the coefficients, generates a global model and broadcasts the global parameters with each client for updating their local models. Finally, the detailed data of SMs remains private. In this paper, we use 5G technologies to facilitate the communication and analysis process of the federated detection. In Fig. 1b, the coloured dashed connections represent the upload flow of training parameters such as weights and gradients from participants to the server. The continuous blue line displays the download link for global model broadcasting. The FL based IDS process includes the following steps:

• First, the concentrator on the server side broadcasts a basic model to initialize the L-IDS of each client.
• Each L-IDS tunes the initial model with training and building its local model on the individual customer’s data. This corresponds to coloured algorithms generated by each L-IDS in Fig. 1b.
• The L-IDSs share the training parameters such as weights, gradients, and biases with the data concentrator through long-range communication technologies over the NAN. Coloured dashed lines in Fig. 1b represent these uploading links per each SM.
• The concentrator on the server side collects all locally trained models and generates a global model by averaging and fusing all collected local models; the averaging process is equivalent to the federated averaging model in Algorithm 1.
• The concentrator now shares this updated model with L-IDSs to upgrade their local algorithms. The blue lines in the architecture depict the downlink connections from the concentrator to each L-IDS, next round, the same process repeats.

It is noteworthy to note that, in the FL concept, every round of training local models, aggregating their parameters, averaging them for the global model generation and consequently receiving updates indicates a communication round.

C. Problem Formulation and Solution

Consider \( m \) participants (households with an implemented IDS), distributed in a neighbourhood, and a server interacting with them. The predicted loss function for each L-IDS with an input sample \( x_i \) and possible output (labelled data) \( y_i \), \( \langle x_i, y_i \rangle, \forall i \in \{1, \ldots, n\} \), with model parameters \( w \) is defined as [28] [30]:

\[
f_i(w) \triangleq \ell(x_i, y_i; w), \quad \forall i \in \{1, \ldots, n\},
\]

The objective is to minimise the total prediction loss of all aggregated local detectors. Hence, the objective function is defined as:

\[
\min_{w \in R^d} f(w) \quad \text{where} \quad f(w) \triangleq \frac{1}{n} \sum_{i=1}^{n} f_i(w),
\]

where \( R^d \) is the real domain value for the parameter model \( w \). The conventional centralised ML scheme aggregates the whole data, \( \{x_i, y_i\}_{i=1}^{n} \), on a central IDS to detect anomalies and trigger the alarm if required. Interestingly, the federated averaging model adds a privacy preservation model in which the real data remains by customers and only learning parameters, i.e. \( w_{\text{c}} \), are aggregated by the central server.

Partitioning the data over \( m \) clients/participants, \( P_m \) can be defined as the set of data points stored on the \( m \)th home/SM. \( \{P_k\}_{k=1}^{m} \) represents the set of data point indices \( \{1, \ldots, n\} \), in which \( n_k = |P_k| \). The objective is to learn a single global model that minimises the empirical risk function over the entire training data set, i.e., to combine the data from all customers. The linear combination of the local empirical objectives is defined as \( F_k(w) \) [28],

\[
f(w) = \sum_{k=1}^{m} \frac{n_k}{n} F_k(w),
\]

where

\[
F_k(w) = \frac{1}{n_k} \sum_{i \in P_k} f_i(w) \quad \forall k \in \{1, \ldots, m\}.
\]

In this paper, the FL mechanism is used to find the optimum empirical value \( F_k(\cdot) \) in each learning duration \( t \). The average loss function of each client/participant \( k \) with the model \( w_k \) can be represented as \( \nabla F_k(w_k) \), where the server updates its global model after aggregating all local models and averaging them using the following equations, 5, 6 as given:

\[
w_{t+1} \leftarrow w_t - \frac{1}{n} \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(w_t),
\]

\[
w_{t+1} \leftarrow w_t - \frac{1}{n} \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(w_t),
\]
Algorithm 1: Federated Averaging IDS Algorithm

\textbf{Input:} \(m\): Total number of L-IDSs, \(T\): Total number of communication interactions, \(E\): local epochs per each interaction.

\textbf{Output:} \(w\)

1: \(t \leftarrow 0\)
2: Server executes: initialize \(w_0\)
3: for each \(t = 1, 2, \ldots, T\) do
4: \(S_t \leftarrow\) Random set of \(k\) L-IDSs
5: for all L-IDSs \(k \in S_t\) do
6: \(w_{t+1}^k \leftarrow\) L-IDS Update \((k, w_t)\) using eq. (5)
7: end for
8: \(w_{t+1} \leftarrow \frac{1}{k} \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k\)
9: end for
10: for each local epoch \(e = 1, 2, \ldots, E\) do
11: \(w \leftarrow \nabla f(x; p)\)
12: end for
13: Return \(w\) to server

where

\[
\sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(w_t) = \nabla f(w_t). \tag{6}
\]

All updates are then applied to models per each L-IDS and the server as \(w_{t+1} \leftarrow w_t - \nabla F_t(w_t)\) and \(w_{t+1} \leftarrow w_t - \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k\).

The federated IDS architecture reported in Fig. 1b provides privacy for customers and decrease high volume data exchange and consequently occupied bandwidth. On the other hand, demand high connectivity for consecutive model exchange between L-IDSs and the neighbour server. In this study, the required steps are presented to implement the gradient federated solution in Algorithm 1. As shown in this algorithm, the server initiates L-IDSs with the initial training parameter \(w_0\), \(k\) set of clients (see lines 1-2). Then, the algorithm updates the training parameters with their local data and generate \(w_{t+1}^k\) (see the internal loop in lines 5-7). Next, the server updates its global values by aggregating all local weights, i.e., \(w_{t+1}\), and training continues for local epoch duration (see global for and line 8). Finally, the proposed approach updates the FL weight values for all the epochs on FL models (see the last for loop in Algorithm 1).

IV. PERFORMANCE EVALUATION

This section evaluates the proposed algorithm against the literature, comparing several evaluation metrics and learning values. In this paper, we implement and evaluate our algorithm on the NSL-KDD train dataset [31]. The NSL-KDD dataset is an improved version of the KDD99 dataset, which is the most widely utilised dataset for anomaly detection evaluation. The attacks in this dataset are classified into four main categories, including Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing Scanning. More details on these attacks and the distribution of each within the dataset are presented in Table II. This dataset can be applied for SG system investigation due to similarities between the SG communication infrastructure and conventional communication technologies in computer networks.

A. Preprocessing

The NSL-KDD dataset includes 40 features, of which three of them are categorical type: protocol type, service and flag. An encoder is required to convert these categorical features into a numerical representation. A straightforward solution is to assign numbers respectively to each category. Although this may seem a simple and efficient solution, the model wrongly interprets a sequential relationship between these classes, and making a fake correlation among the training data compared with other encoding models. To avoid this, we employed a one-hot encoding model to convert these categorical features into numbers. A vector with the same size of classes is assigned to every categorical feature in the one-hot encoding approach. The vector contains ones for the corresponding category and zeroes for all other classes. Although this model can help to distinguish categorical features well, it increases the number of features.

This massive volume of features increases the training time and computational complexity of the system. This also decreases intrusion detection efficiency due to space and capacity limitations of SMs as local processors. We implemented the Recursive Feature Elimination (RFE) method to eliminate redundant features and make the model efficient. The FIDS model includes 16 participants distributed in a neighbourhood, each participant represents a household, and the neighbour’s concentrator is responsible for aggregating the corresponding area’s information. The NSL-KDD training dataset is split randomly among participants to build the required distributed training dataset. Each L-IDS implemented on the SMs by households trains a local model on its data partition after being initiated by the server; the L-IDS builds the training parameters and shares these initial measurements to the server side for building the global model based on formulations provided in section III-C.

The core detector of the FIDS is a five-layered DNN classifier which is called FDNN (Federated DNN), which represents distributed DNN models performing under a federated system. The layers include one input, one output, and three dense layers. Other training parameters are as follows:

1) Optimiser: A federated averaging algorithm in an FL system requires two optimisers: the server optimiser and the client optimiser. This work uses the Adamax optimiser to
be much more flexible and less sensitive to hyperparameters’ choice.

2) Activation function: In all neural network schemes, every node requires an activation function to define that node’s output. Rectified linear unit (Relu) is a widespread and fast activation function prone to saturation for positive values. However, the Relu activation function is not perfect, and it faces the problem of dying nodes, i.e. some nodes stop responding during training. In this paper, the Leaky Relu activation function is utilised to cope with the dying neurons problem, while the SoftMax activator is used in the output layer, i.e. the classifier layer.

Other training parameters are as followed: batch-size = 20, number of epochs = 50 (local on each L-IDS), 70 neurons in the first dense layer, 200 in the second layer, and 20 in the last dense layer. The output includes neurons representing five output categories, four attack classes, and the normal samples. The algorithm runs for 200 iterations (in the FL concept, including 200 communication interactions between clients and the server side). The proposed federated model’s performance was examined by building centralised architecture with various classification algorithms and comparing them with various metrics. The proposed FIDS model trains a DNN algorithm on each L-IDS in this system and average them in a federated manner. To make the comparison easier, we use the term FDNN in the simulation phase to emphasise its federated architecture and DNN based learning model. We also compare FDNN performance with Centralised DNN (CDNN), Support Vector Machine (CSVM), K-Nearest Neighbourhood (CKNN) and Logistic Regression (CLR).

![Fig. 2](image1.png)

**Fig. 2:** Accuracy observation among various algorithms.

![Fig. 3](image2.png)

**Fig. 3:** The comparison of FPR values for different feature numbers among the classifications algorithms. FPR: False Positive Rate.

### TABLE III: Algorithms comparisons on confusion matrix metrics.

<table>
<thead>
<tr>
<th>IDS Algorithms</th>
<th>Evaluation Metrics (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TP</td>
</tr>
<tr>
<td>CDNN</td>
<td>99.52</td>
</tr>
<tr>
<td>CSVM</td>
<td>99.32</td>
</tr>
<tr>
<td>CKNN</td>
<td>99.28</td>
</tr>
<tr>
<td>CLR</td>
<td>96.44</td>
</tr>
<tr>
<td>FDNN</td>
<td>99.55</td>
</tr>
</tbody>
</table>

**B. Evaluation metrics**

In a ML-based model, there are different parameters to evaluate the system’s performance.

- **True Positive (TP):** A true positive rate refers to the percentage of attacks correctly categorised as positive.
- **True Negative (TN):** The classifier’s number of normal samples is correctly diagnosed.
- **False positive (FP):** This number reflects the number of non-attack samples that were incorrectly labelled as attacking samples.
- **False Negative (FN):** It indicates how many attacks are identified as normal samples.
- **Accuracy:** It is used to evaluate the performance of ML models and represents the ratio of correct predictions.
- **Precision:** It is also called specificity, which is the number of correctly predicted positive examples divided by the total number of positive examples.
- **Recall:** It is also called sensitivity representing how many samples were correctly categorised as positive (attack instances) by the algorithm.
- **F1-score:** It combines precision with recall, which makes it a useful metric for comparing classifiers.
- **Area Under the Curve (AUC):** It is the measure of a classifier’s ability to categorise various classes.

**C. Numerical results**

In this section, we propose the method that applies for detecting anomalies corresponding to the NSL-KDD dataset. We evaluate the FDNN model with different evaluation metrics and comprehensively compare its performance against other algorithms.

Fig. 2 illustrates the summary of classifiers’ accuracy impacted by the number of selected features for our federated based detection algorithm and other centralised IDS systems. The number of features has been extended after applying one-hot encoding, as discussed in section IV-A. This figure
first depicts that our model outperforms the CSVM, CKNN and CLR classifiers in terms of accuracy very well. Also, our proposed model can competitively follow the CDNN. Considering the accuracy results in Fig. 2, it is apparent how the proposed method has successfully achieved an accuracy rate of approximately 99.55% by only 60 features out of 122 (extended number of features after encoding).

Also, Fig. 3 illustrates the FP Rate (FPR), per various feature numbers for all classifiers. FPR can lead to higher false alarm rates, so it is an essential criterion to be considered. Under normal working conditions, if the system moves to an attacked state incorrectly, it incurs costs. Apparently, the lower the FPR, the better the classifier’s performance. This figure reveals the descending process of FPR as feature numbers increase. Our FDNN model performs better than other classifiers. Figs. 2 and 3 show the maximum accuracy with a satisfactory FPR in the FDNN is achieved using only 60 features. Applying RFE, we reduce the number of features to 60 most correlated features. We set up the following simulation results based on 60 features.

Within the federated detection scheme, the L-IDS installed by each HAN interacts with the neighbour server in the network to update the training model in every communication round. Fig 4a represents the accuracy evolution of the model per 200 communication rounds. The FDNN classifier of FIDS achieves 99.55% of accuracy within the detection process, which is a very acceptable result for IDS models. Fig. 4b demonstrates the descending procedure of prediction loss compared with accuracy increase per interaction. The gradual reduction of the loss ensures that our algorithm has learned the model and avoids being overfitted. Finally, Fig. 4c presents the time and computation complexity of the system. The time duration per each communication round, i.e. *end_to_end delay*, per different feature numbers increases with the increasing number of features for training. With obtaining 60 features, the end-to-end time duration is reduced, from 140.33 seconds to 129.97 seconds.

Fig. 5 demonstrates the precision (specificity), recall (sensitivity) and f1-score values for the different algorithms. In this figure, the proposed FDNN algorithm outperforms other algorithms in all evaluated metrics. Table III also provides more detailed information on the true positive, false positive, true negative, false negative and AUC metrics. Based on the results, the federated based model performs better in distinguishing normal traffic from attacked ones. Specifically, the FN rate is of great importance for IDS design, as it represents the rate of abnormal data which the classifier missed detection. The AUC result also demonstrates the better performance of the FDNN scheme compared with other classifiers.

However, when discussing a well-designed IDS, the classification of various attacks is also essential. As strategies for the post-attack state and mitigation actions are different for
how FIDS can cope with scarce samples compared with other
50% recall, and 60% f1-score. These results reveal
also performed acceptably in U2R attack detection with 75%
limited samples
This category well, considering its limited samples
NSL-KDD dataset is not balanced well and lacks sufficient
each attack category. Table IV demonstrates the classification
and other central IDS algorithms. Based on the classification
our approach could perform very well in almost all classes compared to other algorithms. Specifically, because the
training phase. While the results reveal our model
also performed acceptably in U2R attack detection with 75%
precision, 50% recall, and 60% f1-score. These results reveal
how FIDS can cope with scarce samples compared with other
models.

V. CONCLUSIONS AND FUTURE DIRECTION

This paper proposed FIDS, an FL detection architecture
based on DNN that delivers SG’s IDS system as a distributed
architecture addressing security and privacy concerns for the
measuring system of SG. In this study, we design a 5G network
infrastructure for the metering system to provide reliable
connectivity and spectrum efficiency for regular communication
among local IDSs on customers’ SMs and the concentrator. The
paper assessed different evaluation metrics and made a
comprehensive comparison against various traditional classi-
fiers to validate the proposed method’s performance. Results
confirm the satisfying achievements of the proposed classi-
fication algorithm, FDNN, in various classification criteria.

The plan is to extend the studied approach to monitor the
traffic over the 5G network for future work. In this way, we
shall build an approach for SMs by monitoring the traffic over
a 5G network and design lightweight cryptography schemes
to secure the ML weights interaction in the federated model.

Also, the resilience of FIDS facing false reports that dishonest
customers may inject into the system should be more investigat-

REFERENCES

[1] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, “Commu-
nication in smart grids: A comprehensive review on the existing and
future communication and information infrastructures,” IEEE Systems
load frequency control in smart grids,” in 2013 IEEE PES Innovative
attacks in smart meter data collection using moving target defense,”
in Proceedings of the 13th ACM Symposium on QoS and Security for
analysis in ai-based smart grid,” in SoutheastCon 2021. IEEE, 2021,
pp. 01–07.
eavesdropping attacks in scada/ics network data streams through impul-
sive statistical fingerprinting,” in International Conference for Emerg-
attacks in smart grid,” in 2016 12th International Conference on Com-
sion detection of cyber physical energy system based on multivariate
anomaly based intrusion detection system,” Materials Today: Proceed-
ings, 2021.
IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1732–
1754, 2014.
tinez, A. Sarigiannidis, G. Efthathopoulos, Y. Spyridis, A. Sesis,
N. Vakakis et al., “Spear siem: A security information and event
management system for the smart grid.” Computer Networks, vol. 193,
[13] V. Mothukuri, R. M. Parizi, S. Fouriyeh, Y. Huang, A. Dehghantanha,
and G. Srivastava, “A survey on security and privacy of federated
2021.
Concept and applications,” ACM Transactions on Intelligent Systems
and Technology (TIST), vol. 10, no. 2, pp. 1–19, 2019.
learning,” Foundations and Trends® in Machine Learning, vol. 14, no. 1,
2021.
grid with supervised learning.” in 2016 International Joint Conference
on Neural Networks (IJCNN). IEEE, 2016, pp. 1395–1402.
“Smarter security in the smart grid,” in 2012 IEEE Third International
Conference on Smart Grid Communications (SmartGridComm). IEEE,
[18] M. Ozay, I. Esnaoila, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor,
“Machine learning methods for attack detection in the smart grid,” IEEE
transactions on neural networks and learning systems, vol. 27, no. 8,
learning-based detection of covert data integrity assault in smart grid
networks utilizing isolation forest,” IEEE Transactions on Information
detection in smart grid: A reinforcement learning approach.” IEEE
attacks in smart grid: A deep reinforcement learning-based approach.”
[22] A. A. Cárdenas, R. Berthier, R. B. Bobba, J. H. Huh, J. G. Jetcheva,
detection architectures in advanced metering infrastructures,” IEEE
influence detection system against false metering attacks in smart grid,” in
IEEE, 2019, pp. 1–6.
for smart grids: Securing power traces in collaborative learning.” arXiv
consumer characteristics identification: A federated learning approach.”
IEEE Transactions on Smart Grid, 2021.
[27] K. Bonawitz et al., “Towards federated learning at scale: System design,
[28] J. Konečný, B. McMahan, and D. Ramage, “Federated optimization:
[29] S. Savazzi, M. Nicolì, and V. Rampa, “Federated learning with cooper-
ating devices: A consensus approach for massive iot networks,” IEEE
[30] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas,
“Communication-efficient learning of deep networks from decentralized
data,” in Artificial Intelligence and Statistics. PMLR, 2017, pp. 1273–
1282.
using various machine learning techniques for intrusion detection.”
International Journal of Engineering Research & Technology (IJERT),