Electricity-Theft Detection for Change-and-Transmit Advanced Metering Infrastructure

Mohamed I. Ibrahem, Mohamed M. E. A. Mahmoud, *Senior Member, IEEE*, Fawaz Alsolami, *Member, IEEE*, Waleed Alasmary, *Senior Member, IEEE*, Abdullah Saad AL-Malaise AL-Ghamdi, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—The periodic transmission of the customers' power consumption readings in the advanced metering infrastructure (AMI) is essential for energy management and billing. To collect the readings efficiently, the change and transmit approach is adopted in AMI (CAT AMI) so that the readings are reported only when there is enough change in the consumption. However, CAT AMI suffers from malicious customers who launch electricity-theft cyberattacks by manipulating their readings to illegally reduce their bills. These attacks can cause hefty financial losses and degrade the grid performance because the readings are used for grid management. In this article, the electricity-theft problem in CAT AMI networks is investigated. We first process a real power consumption readings data set to create a benign data set and propose a new set of cyberattacks to create malicious samples. We then develop a deep-learning-based electricity-theft detection solution to identify malicious customers for the CAT AMI network. The proposed detector uses both the customers' transmission pattern and CAT readings to learn the correlation between them in order to enhance the detector's ability in identifying electricity thefts. We conduct extensive experiments to evaluate the performance of our electricity-theft detector, and the results indicate that our detector can accurately detect malicious customers and achieve higher detection rate and lower false alarm than the detectors that are trained only on the CAT readings.**

***Index Terms*—Change and transmit approach is adopted in AMI (CAT AMI) network, electricity-theft cyberattacks, electricity-theft detection, smart grid (SG).**

Manuscript received 14 March 2022; revised 26 May 2022 and 4 July 2022; accepted 25 July 2022. Date of publication 17 August 2022; date of current version 7 December 2022. This work was supported by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, under Grant KEP-18-611-42. *(Corresponding author: Mohamed M. E. A. Mahmoud.)*

Mohamed I. Ibrahem is with the Department of Cyber Security Engineering, George Mason University, Fairfax, VA 22030 USA, and also with the Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11672, Egypt (e-mail: mibrahem@gmu.edu).

Mohamed M. E. A. Mahmoud is with the Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN 38505 USA (e-mail: mmahmoud@tntech.edu).

Fawaz Alsolami is with the Department of Computer Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: falsolami1@kau.edu.sa).

Waleed Alasmary is with Communication and Information Technology Commission, Riyad 12382, Saudi Arabia (e-mail: wsasmary@gmail.com).

Abdullah Saad AL-Malaise AL-Ghamdi is with the Information System Department, King Abdulaziz University, Jeddah 21341, Saudi Arabia, and also with the Information Systems Department, HECI School, Dar Alhekma University, Jeddah 22246, Saudi Arabia (e-mail: aalmalaise@kau.edu.sa; aghamdi@dah.edu.sa).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Digital Object Identifier 10.1109/JIOT.2022.3197805

I. Introduction

MOST of the countries all over the world started to implement a smart grid (SG) infrastructure because it creates a reliable, clean, and efficient power system compared to the traditional power grid [1]. SG contains an advanced metering infrastructure (AMI) which comprises of a set smart meters (SMs) deployed at the homes of the customers. AMI enables collecting SMs' power consumption readings by the electric utility (EU) for energy management, load monitoring, billing computation, etc. [2].

Basically, there are two approaches to collect the SMs' power consumption readings in SG: 1) periodic transmission (PT) [1], [2], [3], [4], [5] and 2) change and transmit (CAT) [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. Using the PT approach, the SMs send the power consumption readings periodically to the EU [3]. However, this approach suffers from transmitting an enormous amount of data between the SMs and EU, especially, after considering the fact that AMI networks have millions of SMs and they are scalable. This undoubtedly causes poor usage of the available resources (bandwidth), especially when transmitting the SMs' readings using cellular networks [4], [5]. On the other hand, the SMs' power consumption readings can be collected more efficiently by using the CAT approach because the readings are sent to the EU only when there is a sufficient change in the consumption compared to the last reported reading [6], [13], [14], [15], [16]. More precisely, a reading is sent when the absolute value of change in the consumption exceeds a predefined threshold. For example, at 10% threshold, each SM reports a reading when the change in the current consumption is above +10% or below −10% of the last reported consumption. If a reading is not sent by an SM, the EU uses the last reading reported by the SM. In this case, we refer to this AMI by "CAT approach is adopted in AMI (CAT AMI)," while we use the term "PT AMI" to refer to the AMI in which the SMs' power consumption readings are transmitted constantly.

Both PT and CAT AMIs are vulnerable to electricity-theft cyberattacks that can be launched by malicious customers who steal electricity by tampering their SMs and reporting lower power consumption readings to reduce their bills illegally. Such attacks may cause severe problems in the existing power grid such as financial losses, e.g., about U.S. $6 billion are lost every year in the United States (U.S.) because of electricity thefts [17]. Also, the developing countries suffer from losses due to electricity thefts, e.g., India loses about U.S. $17 billion annually [18]. Moreover, this deceptive behavior may affect the stability of the grid or cause blackout in the worst cases since the false readings reported by malicious customers are used for energy management and load monitoring [19].

Different machine learning-based electricity-theft detectors have been proposed in the literature to identify malicious customers in the AMI networks [18], [20], [21], [22], [23], [24]. Some of these detectors are based on deep learning models [20], [23], [24], while other detectors are based on shallow models [18], [21], [22]. Among the existing detectors, most of these works have demonstrated that the deep-learning-based electricity-theft detectors can accurately detect electricity thefts. However, all the existing electricity-theft detectors are developed for the PT AMI networks, and none of the existing works has investigated the problem of electricity theft in CAT AMI networks.

Detecting electricity-theft cyberattacks in the CAT AMI network is different from that of the PT AMI for the following reasons. In case of the PT AMI, the SMs send their power consumption readings at each time slot, i.e., periodically, to the EU which receives all the readings and run electricity-theft detector. Hence, the detector in the PT AMI is trained on accurate readings (i.e., customers' fine-grained power consumption readings) to learn their consumption patterns and use them to detect malicious customers. However, in the case of CAT AMI, the problem becomes more complex because the readings in this case are clipped due to using the threshold of the CAT approach in transmitting the readings which makes the readings noisy. When an SM does not report a reading, the EU uses the last reading reported by the SM for the electricity-theft detector evaluation. This means that a new data set for the CAT AMI that contains CAT power consumption readings and a new detection approach are required to be able to detect electricity-theft cyberattacks accurately in the CAT AMI.

Moreover, new attacks tailored to the CAT AMI should be investigated because CAT AMI readings may be lower than the actual readings and this may be exploited by the attackers to craft stealth electricity-theft attacks. On the other hand, the attacks against the PT AMI aim at reducing the readings while attempting to imitate the consumption pattern to avoid being detected, and in this case, the attacker guarantees that there is a reduction in his/her bill, whereas, when reporting false readings in CAT AMI, the attacker should also follow the CAT approach by sending a reading only if the consumption change exceeds a predefined threshold; otherwise, the attack can be easily detected. In other words, the attacker needs to consider the threshold of the CAT approach in computing the false readings and also make sure there is a reduction in his/her bill. This is because the reported reading, that is considered by the EU for billing, may be greater than the current consumption when the absolute value of change in the consumption does not exceed the threshold and, hence, there is no bill reduction in this case. In addition, simple attacks, e.g., reporting zero readings, have been used in most of the existing research works in the PT AMI [18], [20], [21], [22], [23], [24], which are easily detectable even without the use of machine learning techniques.

Therefore, we investigate, in this article, the detection of malicious customers who report false electricity consumption readings to reduce their bills in the CAT AMI network using different machine learning-based detectors. Our methodology starts with preparing the data set followed by the design of the electricity-theft detector, and finally the evaluation of the detector's performance. We create a new data set for CAT AMI by considering different thresholds using a real power consumption data set which is provided by the Smart project [25]. This data set contains only real benign power consumption readings and is used to train and evaluate our electricity-theft detectors. Next, to create malicious samples for CAT AMI, we propose a set of new attacks that are tailored to CAT AMI to imitate the behavior of malicious customers. Finally, we propose a general electricity-theft detector using a hybrid deep learning model to detect malicious customers with high accuracy.

Our detector is general in the sense that it shall be used for all customers. It is a hybrid deep learning model that uses a gated recurrent unit neural network (GRU), fully connected feedforward neural network (FFN), and a convolutional neural network (CNN). The CNN and GRU are used in our detector to extract the important features in the input CAT readings and capture the complex correlation between the extracted features, respectively. In addition, the FFN is used to make accurate classifications. Furthermore, our detector processes the transmission pattern of the customers besides the CAT readings to boost the performance of the detector since the transmission pattern may change when a customer reports malicious consumption readings. The transmission pattern contains a set of binary numbers in which each number corresponds to a reporting period, where it is one in case of transmitting a reading while it is zero in the case of no transmission. When the attacker reports false reading, he/she should follow the CAT approach by making sure that the readings follow the predefined threshold; otherwise, he/she can be detected easily. Moreover, the transmission pattern contains information about the customer's behavior that the electricity-theft detector needs to learn to differentiate between the malicious and benign customers. Thus, considering the transmission pattern in addition to the CAT readings can further enhance the detector's ability to identify malicious customers. The results of our experiments show that the proposed detector can detect electricity-theft cyberattacks with higher accuracy and performance than the detector that is trained solely on the CAT readings.

To the best of our knowledge, this is the first work that investigates the electricity-theft detection in the case of CAT AMI networks, and in order to achieve this objective, we have done the following phases.

1) Benign data sets for CAT power consumption readings at different predefined threshold values have been created. Then, we propose new attacks that are tailored to CAT AMI to create malicious samples.
2) We train a hybrid and multi-input deep-learning-based electricity-theft detector to identify malicious customers

for the CAT AMI network. Our detector uses the customer's transmission pattern in addition to the CAT readings to enhance the detector's performance.

3) We conduct extensive experiments to evaluate the performance of our electricity-theft detector, and the results indicate that our detector can accurately detect malicious customers. Furthermore, it outperforms the detectors that are trained solely on the CAT readings in terms of detection rate and false alarm.

The remainder of this article is as follows. The existing works in the literature that investigate detecting electricity theft in AMI networks are discussed in Section II. Then, our considered system models are delineated in Section III. Next, Section IV presents the data set created for training and evaluating our detectors. A brief description of several classifiers that use different machine learning models to detect malicious customers is discussed in Section V. The proposed electricity-theft detector is presented in Section VI. Then, the performance evaluation of our detector is discussed in Section VII. Finally, the conclusions are drawn in Section VIII.

II. Related Work

This section discusses the research works that investigate the detection of malicious customers who launch electricity-theft cyberattacks to steal electricity by reducing their bills for the AMI networks of the smart power grid. Next, we will discuss their shortcomings and research gap.

A. Electricity-Theft Detection in Periodic Transmission AMI

In the literature, different machine learning-based electricity-theft detectors have been proposed for the PT AMI networks to identify malicious customers who launch electricity-theft cyberattacks [18], [20], [21], [22], [23], [24]. Some of these detectors are based on deep learning models [20], [23], [24], while other detectors are based on shallow models [18], [21], [22]. In this section, we survey these solutions.

1) Shallow Detectors: Ford *et al.* [21], Buzau *et al.* [22], and Yan and Wen [26] have proposed electricity-theft detectors. While the proposed detector in [21] uses a single hidden layer artificial neural network, both detectors in [22] and [26] are based on extreme gradient boosted trees (XGBoost). These detectors are general in the sense that they can be used for all customers since they are trained on the data of a large number of customers. Thus, they have several advantages. First, they can be used for new customers who do not have a history of power consumption. Second, low computation power is needed because a general detector is trained for all customers instead of training one detector for each customer. In [21], a load predictor is used to create an electricity-theft detector in which the detector uses the previous power consumption readings to predict the future consumption values and then compare them to the reported readings. Then, if the difference between the predicted and reported readings does not exceed a certain value, the customer is identified as honest; otherwise, he/she is identified as malicious. Unlike the proposed detector in [21] that is trained only on benign readings, the electricity-theft detector proposed in [22] is trained on malicious and benign samples which are available in the data set of Endesa [24].

Jokar *et al.* [18], Ford *et al.* [21], and Yan and Wen [26] have used the Irish data set [27] which contains real and benign power consumption readings samples to train the electricity-theft detectors. Unlike the proposed detectors in [22], [26], and [21] that train general detectors, the detector in Jokar *et al.* [18] is customized, i.e., a detector is trained for each customer using his/her power consumption readings. Two experiments were conducted in [18] to train electricity-theft detectors. The first experiment trains a support vector machine (SVM)-based detector using only the benign samples for each customer while the second experiment trains an SVM detector using malicious and benign samples. Jokar *et al.* [18] introduced a set of attacks to create synthetic malicious samples since the Irish data set does not contain malicious samples. The results in [18] indicate that the detector that is trained on both types of samples offers better performance than the detector that is trained only on benign samples.

Although these studies have indicated that the XGBoost-based electricity-theft detector offers better performance compared to SVM, K-nearest neighbors detectors, and logistic regression, the shallow-based detectors do not exploit the temporal correlation of the power consumption readings, and better performance can be obtained if the detector can learn the temporal correlation.

2) Deep-Learning-Based Detectors: Since the shallow-based electricity-theft detectors do not provide high performance, the proposed detectors in [20], [23], and [24] use deep learning because of its ability to better capture the temporal correlations and extract the important features of the electricity consumption readings. Various deep-learning-based detectors are trained in [23] using a synthetic data set. These detectors are general and use CNN, stacked autoencoder, and long short-term memory network (LSTM). Moreover, the performance of these detectors is compared to shallow detectors including shallow NN, random forest (RF), and decision tree (DT). The results demonstrate that the detectors which use deep learning architectures give better performance than the shallow detectors.

General electricity-theft detectors have been trained in [20] and [24] using state grid corporation of China (SGCC) [28] and Endesa [24] data sets, respectively. The SGCC data set contains both malicious and benign samples. The proposed detector in [20] is based on a deep learning architecture which consists of CNN and multilayer perceptron (MLP) components to be able to capture the periodicity of electric consumption readings since according to a statistical analysis that is carried on the SGCC data set, it has been observed that the electricity consumption readings of malicious customers are usually less periodic or nonperiodic compared to that of normal customers. The proposed detector learns the temporal correlation of the time-series electricity consumption readings to detect false readings reported by malicious customers. Moreover, the proposed deep-learning-based detector in [24] composes of MLP and LSTM modules. The results show that the proposed detector outperforms the detector of [20] in terms of the detection accuracy. Most of these studies have indicated that utilizing the fine-grained energy consumption readings with deep-learning-based models can accurately detect electricity thefts.

B. Limitations and Research Gap

As can be noticed from the previous section, all the existing works consider only detecting electricity-theft cyberattacks in the PT AMI networks, and the detection of electricity theft in the CAT AMI has not been investigated yet. The CAT approach is an efficient data collection method for AMI network of the SG that has been adopted and investigated by several works in the literature [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. Some of these works investigated different applications in SG, e.g., demand/response [7] and load disaggregation [8] while using the CAT approach, while the other works in [9], [10], [11], and [12] focus on finding a good threshold value for the consumption change that triggers transmitting a reading. All of these works do not consider that there may be malicious customers who may report false readings to reduce their bills illegally. Therefore, in this article, we investigate different methods to detect electricity theft for the CAT AMI using a publicly available data set that contains real power consumption readings in order to fill the research gap. Moreover, we propose a hybrid and multi-input deep-learning-based electricity-theft detector to detect malicious customers for the CAT AMI network with high detection performance.

The detection of electricity-theft cyberattacks in the CAT AMI network is different from that of the PT AMI for the following reasons. In case of the PT AMI, the SMs sends their power consumption readings at each time slot, i.e., periodically, to the EU which receives all the readings and run electricity-theft detector. Hence, the detector in the PT AMI is trained on accurate readings (i.e., customers' fine-grained power consumption readings) to learn their consumption patterns and use them to detect malicious customers. However, in the case of CAT AMI, the problem is more complex because the readings in this case are clipped due to using the threshold of the CAT approach in sending the readings which introduces inaccuracy (or noise) to the data. When an SM does not report a reading, the EU should use the last reported reading for the electricity-theft detector evaluation. This means that a new data set for the CAT AMI that contains CAT power consumption readings and a new detection approach are required to be able to detect electricity-theft cyberattacks in the CAT AMI. What makes the problem more challenging is that a general detector needs to be devised so that it can be used for all customers. This can be done by training it on data from various customers who have different consumption profile and, thus, different CAT readings and transmission patterns.

Moreover, new attacks tailored to the CAT AMI should be investigated because CAT AMI readings may be lower than the actual readings and this may be exploited by the attackers to steal electricity without being detected. On the other hand, the attacks against the PT AMI aim at reducing the readings while attempting to imitate the consumption pattern to avoid being detected, and in this case, the attacker guarantees that there is a reduction in his/her bill, whereas, when reporting false readings in CAT AMI, the attacker should also follow the CAT approach by sending a reading only if the consumption change exceeds a predefined threshold, otherwise, the attack can be easily detected without the need for machine learning models. In other words, the attacker needs to consider the threshold of the CAT approach in computing the false readings and also make sure that there is a reduction in his/her bill. This is because the reported reading, that is considered by the EU for billing, may be greater than the current consumption when the absolute value of change in the consumption does not exceed the threshold, and in this case, there is no bill reduction. In addition, most of the existing research works in the PT AMI have introduced simple attacks, e.g., sending zero readings [18], [20], [21], [22], [23], [24], which is easily detectable even without the need for machine learning methods. Therefore, we introduce, in this article, a set of sophisticated attacks that take the threshold of the CAT approach into account and attempt to imitate the pattern of CAT readings to avoid being detected while ensuring that there is a bill reduction.

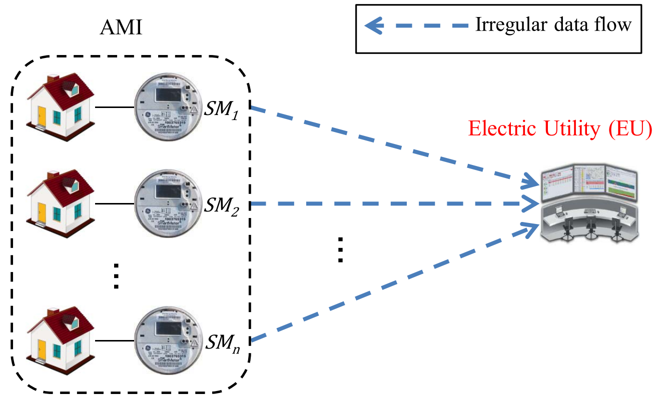


Fig. 1. Network model for electricity-theft detection for the CAT AMI network.

III. Network and Threat Models

This section discusses the network and threat models considered in this article.

A. Network Model

As shown in Fig. 1, the main entities of the AMI network considered in this article include a set of SMs and the EU. The SMs are installed at the customers' premises to send real-time power consumption readings to the EU using CAT approach, i.e., sending a reading if a sufficient power consumption change compared to the last reported reading occurs. In other words, the SMs do not send the consumption in some time slots, and they only send the power consumption readings when the absolute value of change in the consumption exceeds a predefined threshold. For example, at 10% threshold, each SM reports a reading when the change in the current consumption is above +10% or below −10% of the last reported consumption. The threshold value is a system parameter which is distributed by the EU to all SMs so that they can use it to transmit their readings based on the CAT approach. The power consumption readings sent by SMs are used by the EU for billing, load monitoring, and energy management. Furthermore, the EU uses these readings to evaluate a machine learning model to detect electricity-theft cyberattacks.

B. Threat Model

The customers may report false power consumption readings to the EU to reduce their bills illegally. This does not only cause financial losses but it may also result in wrong decisions regarding energy management. This misbehavior can be done by compromising the SMs and reprogramming them to launch electricity-theft cyberattacks by reporting false readings to the EU [29]. To compromise an SM, the SM's software can be modified or a malicious software can be programmed and installed on it to be accessed through an ANSI optical port [30]. Furthermore, some platforms, e.g., Terminator, can be used to hack the SMs by guessing the passwords. In addition, according to [31], electricity-theft cyberattacks may be launched by attacking the communication network since it has been found that there are vulnerabilities in the communications of AMI networks. Moreover, adversaries in the system can collude together if this can help to launch successful electricity-theft attacks. Each SM shares a secret key with the EU and uses it to encrypt the power consumption readings to protect their confidentiality and integrity.

IV. Data Set Preparation

This section presents the power consumption data that is used to train and evaluate our electricity-theft detectors. We use real benign power consumption readings from a publicly available data set [25] to create a data set for CAT AMI using different thresholds. To create malicious samples, a set of electricity-theft cyberattacks that can be launched by malicious customers are proposed. Finally, we will discuss how the benign and malicious data sets can be used to train our detectors.

A. Benign Data Set

In this article, a publicly available real SM data set is used for preparing our data set. This data set is provided by the Smart project [25]. It includes real and benign power consumption readings for 114 households in 2016, in which a power consumption reading is reported to the EU every minute. From this 1-min granularity data set X_{SM} and by summing up the consumption readings, we have created two data sets X_{SM}^{5} and X_{SM}^{10} with transmission rates of 1/5 min (i.e., 288 readings per day) and 1/10 min (i.e., 144 readings per day), respectively, where "1/t min" denotes the transmission rate which means one reading is reported every t minutes, and t is the transmission interval. Hence, based on a data set of real benign CAT readings from 114 customers over 349 days, the daily readings are considered a benign sample with a total of 39 786 (114×349) samples. Each sample contains 288 and 144 CAT readings for transmission rates of 1/5 and 1/10 min, respectively.

TABLE I
Saving (%) Achieved by Using CAT Approach at Transmission Rates and Different Thresholds

		Threshold (%)	
		5	10
Transmission rate	1/5min	36.48	39.75
	1/10min	19.95	25.87

Next, we used X_{SM}^{5} and X_{SM}^{10} to create other data sets for the CAT approach at thresholds of 5% and 10%. This means that by using 10% threshold, a power consumption reading is sent by the SM only when the absolute value of change in the consumption exceeds 10%. We measured the saving that is achieved due to using the CAT approach in terms of the percentage of unreported readings comparing to sending the readings periodically at different transmission rates and thresholds by using the following formula:

$$\text{Saving} = \frac{N_P - N_C}{N_P} \times 100$$

where N_C is the number of transmitted readings in case of CAT approach while N_P is the number of transmitted readings in case of PT of the readings. The bandwidth saving that is achieved due to using the CAT approach is given in Table I at different transmission rates and thresholds. It can be noticed that the saving increases as the threshold increases because the likelihood that the consumption change exceeds the threshold of the CAT approach decreases, which consequently leads to fewer number of transmissions. On the contrary, the saving decreases as the transmission interval increases because the likelihood that the consumption change exceeds the threshold increases, which causes more transmissions.

Since the EU receives clipped power consumption readings (CAT readings) from the SMs because of using the CAT approach, a reading error may occur due to the fact that the reading taken into account by the EU may be greater (or less) than the actual reading measured by the SM due to the use of a threshold. Since the EU computes the aggregated reading of a group of SMs for load monitoring and the aggregated reading of a set of readings of each customer for billing, the aggregated reading error is calculated using our data sets assuming that the AMI network has 114 SMs. Therefore, the cumulative distribution function (CDF) of the aggregated reading error for load monitoring is shown in Fig. 2 at different transmission rates and thresholds. In addition, we also plot, in Fig. 3, the error in the aggregated reading for billing of two randomly selected customers over a year. As we can see from these figures, the aggregated reading error is significantly less than the maximum individual readings' error (the threshold value) because some errors are positive and other errors are negative, which can reduce the error of the aggregated reading. Therefore, although the readings that are received by the EU, i.e., CAT readings, are clipped, the EU can still use

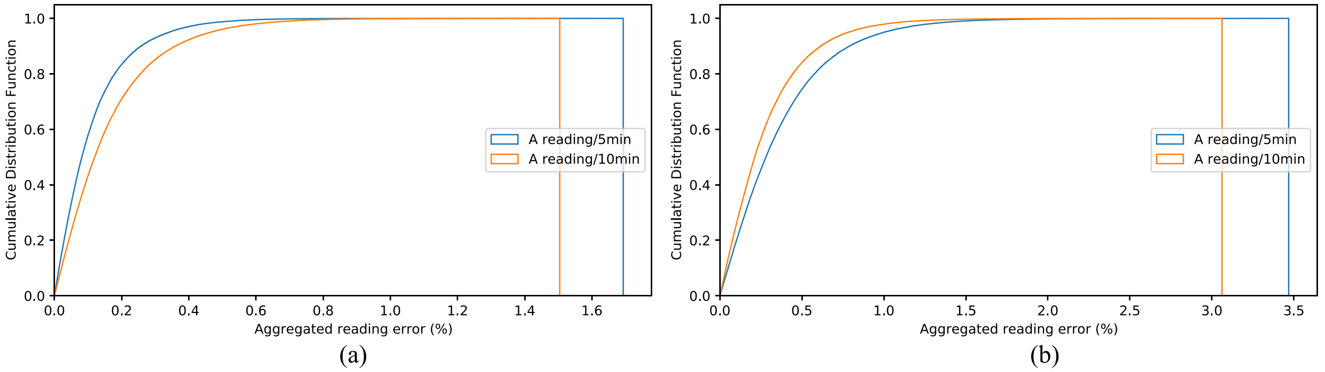


Fig. 2. CDF of the error in the aggregated reading for load monitoring at different thresholds and transmission rates. (a) At 5% threshold. (b) At 10% threshold.

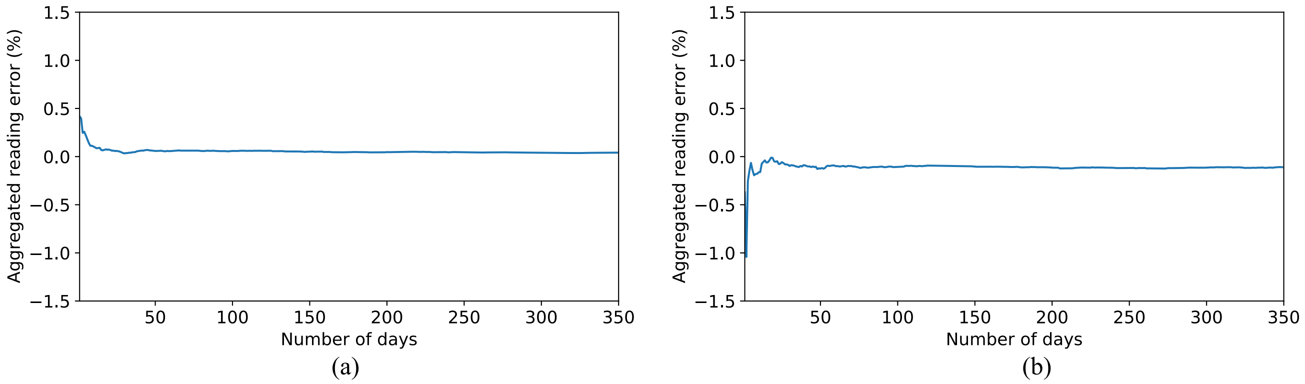


Fig. 3. Aggregated error for billing of two randomly selected customers over a year. Aggregated error of (a) customer 1 and (b) customer 2.

them for billing and load monitoring accurately. Based on the information given in Figs. 2 and 3, and Table I, we decided to choose threshold values of 5% and 10% since these values offer a reasonable saving in the bandwidth with acceptable error.

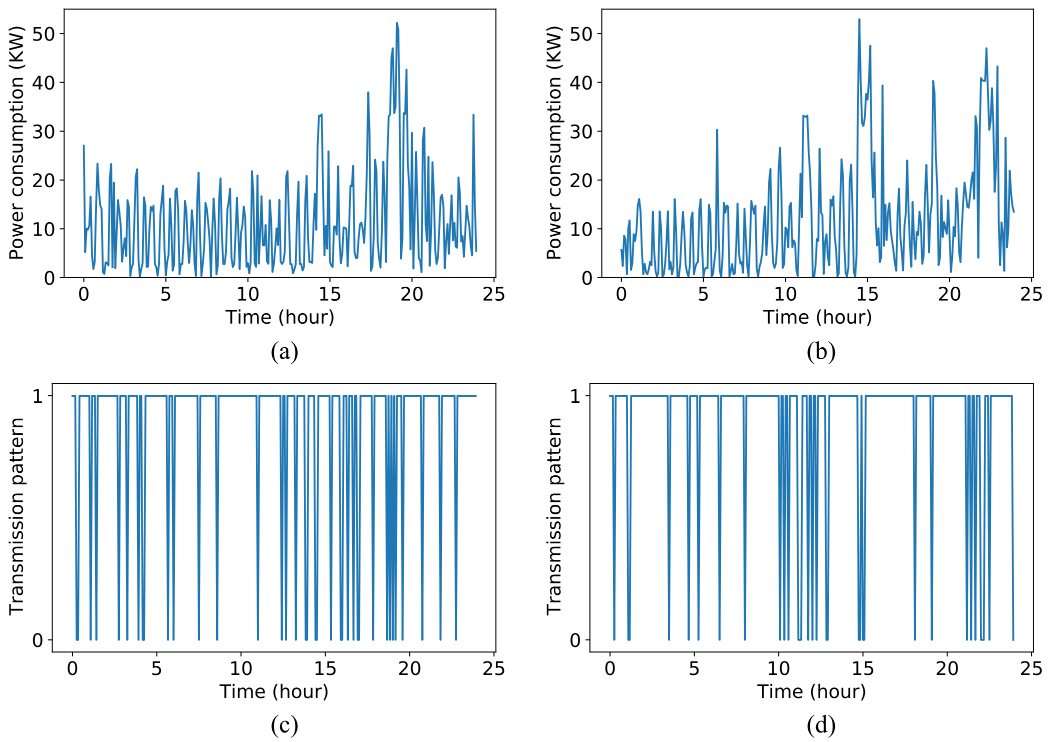
We visualized our data set to gain better insights by displaying the data in a visual context so that CAT transmission patterns can be explored. Fig. 4 shows the real power consumption and the corresponding transmission patterns due to using CAT approach of two customers which are selected randomly from our data set. As can be seen from Fig. 4(c) and (d), there are no transmission events at certain periods because readings do not pass the threshold. In other words, at these periods, the change in the consumption does not exceed the threshold, and in this case, the EU should use the last reported reading. This means that the real reading may be lower than or higher than the corresponding CAT reading.

B. Malicious Data Set

Since we need to train our electricity-theft detectors using both benign and malicious data samples and due to the lack of real malicious samples for the CAT AMI, we propose a set of attacks that can be launched in the CAT AMI network to mimic the attacks of malicious customers to create malicious samples. For those customers to launch electricity-theft cyberattacks to reduce their bills, they need to lower the values of the readings that they report while following the CAT approach, i.e., the readings reported by the SMs should respect the predefined threshold of the CAT approach. Without following the CAT approach, these attacks are easily detectable even without the need for machine learning-based electricity-theft detection methods because the EU can simply compare the readings sent by the SMs and their last reported readings and check whether the reported readings exceed the threshold.

In order to generate malicious samples, we propose five attacks and apply them on benign samples. The proposed attacks are summarized in Table II. As can be seen from the table, each attack function $f(\cdot)$ aims at achieving a reduction in the bill by applying different attack scenario. Denote r_c^i and r_l^i as the current true electricity consumption and the last reported reading of SM_i, respectively. Let Th_{act} be the actual threshold of the CAT approach, and to send a reading, the following condition should be achieved $r_c^i < x_l^i$ or $x_u^i < r_c^i$, where $x_l^i = r_l^i - (r_l^i * \text{Th}_{\text{act}})$, $x_u^i = r_l^i + (r_l^i * \text{Th}_{\text{act}})$, and x_l^i and x_u^i are the lower and upper limits, respectively.

As shown in Table II, Attack 1 reduces the first reading when launching the attack by η%, and then follows the rate of change of the true readings to compute the malicious readings. This means that if the consumption of a time slot increases/decreases by percentage p comparing to the last reading, the attacker increases/decreases the malicious readings by the same percentage p. The objective of this attack is to make the malicious consumption pattern look like the real pattern but with lower magnitudes to confuse the detector. Also, this



(a) (b) (c) (d)

Fig. 4. Real consumption and transmission patterns due to using CAT approach of different customers, where in (c) and (d), 1 and 0 refer to transmission and no transmission events, respectively, at 1/5-min transmission rate and 10% threshold. Real power consumption pattern of (a) customer 1 and (b) customer 2. Transmission pattern of (c) customer 1 and (d) customer 2.

TABLE II
PROPOSED CYBERATTACK FUNCTIONS FOR ELECTRICITY THEFT FOR CAT AMI

Attacks	Attack function
Attack 1	$f_1(r_c^i) = \begin{cases} \eta \times r_c^i & \text{If first reading} \\ (1+p) r_l^i & otherwise \end{cases}$
Attack 2	$f_2(r_c^i) = \begin{cases} r_c^i & r_c^i < x_l^i \text{ or } r_l^i < r_c^i < r_{c-1}^i \\ r_l^i & otherwise \end{cases}$
Attack 3	Choose asymmetric thresholds Th_l and Th_u, where $Th_l = Th_{act}$ and $Th_u = Th_{act} \times \alpha_u + Th_{act}$ $f_3(r_c^i) =$ $\begin{cases} \text{Do not transmit} & r_l^i - r_l^i * Th_l < r_c^i < r_l^i + r_l^i * Th_u \\ \text{Transmit } r_c^i & otherwise \end{cases}$
Attack 4	$f_4(r_c^i) = \alpha_c \mathbb{E}[\boldsymbol{r}_d^i]$
Attack 5	$f_5(r_c^i) = \beta_c r_c^i$

attack aims to make the transmission pattern look similar to the true pattern to confuse the detector.

In Attack 2, the attacker sends r_c^i when: 1) r_c^i is less than x_l^i and 2) r_c^i is greater than r_l^i and less than the previous reading r_{c-1}^i. Hence, in this attack, the EU uses the last reported reading r_l^i when $x_u^i < r_c^i$ instead of considering the actual current consumption r_c^i which is higher than x_u^i. Also, this attack aims at confusing the electricity-theft detector while achieving a reduction in the bill since some readings are true (when $r_c^i < x_l^i$ or $r_l^i < r_c^i < r_{c-1}^i$), while others are false (when $r_c^i < x_u^i$).

On the other hand, in Attack 3, instead of following the symmetric threshold Th_{act}, i.e., ±10%, the attacker creates and follows asymmetric threshold Th_l and Th_u, e.g., $\text{Th}_l = 10\%$ and $\text{Th}_u = 20\%$, where Th_l and Th_u are the lower and upper limits of the attacker's threshold, respectively, and $\text{Th}_l = \text{Th}_{\text{act}}$. In this attack, the attacker randomly chooses Th_u so that $|\text{Th}_l| < |\text{Th}_u|$ to ensure a reduction in the bill and a reading is transmitted when $r_c^i < r_l^i - r_l^i * \text{Th}_l$ or $r_l^i + r_l^i * \text{Th}_u < r_c^i$. Moreover, as Th_u increases, as the probability that the current consumption exceeds the upper limit decreases and, hence, the EU uses the last reported consumption r_l^i, which is lower than the current consumption r_c^i, to lower the bill. In other words, the current consumption, which is bigger than the last reported reading, is transmitted only when there is a large difference between the last reported reading and the current consumption, which guarantees a reduction in the bill. By launching Attack 3 continuously, the EU may observe that the change in the transmitted readings comparing to the last reported readings is always above Th_u (or the number of transmissions is below the average value). Therefore, this attack should be launched for certain time periods to prevent the EU from observing that the change in the transmitted readings are always above Th_u. Also, due to the natural randomness in the transmission pattern due to the randomness of the activities of the dwellers, depending only on the number of transmissions to detect electricity theft would give inaccurate detection results with high false alarms.

The objective of Attacks 4 and 5 is to scale down all the consumption readings by a ratio and then follow the CAT approach correctly in transmitting the readings. Attack 4, i.e., $f_4(\cdot)$, computes the mean value $\mathbb{E}[\boldsymbol{r}_d^i]$ of a fraudulent customer's power consumption readings for a given day d, and reduces it using a time-dependent ratio α_c. Attack 5 $[f_5(\cdot)]$ reduces each power consumption r_c^i by a time-dependent ratio β_c, where $0 < \alpha_c < 1$ and $0 < \beta_c < 1$.

Note that all these attacks should follow the CAT approach in which a reading is transmitted only when the consumption change exceeds the threshold Th_{act} because the attacker can be detected by the EU if the reported readings do not follow the threshold Th_{act}.

C. Data Preprocessing

To use the aforementioned attacks to produce malicious samples, we first set the parameters of each attack function, if applicable. In order to simulate different malicious behaviors, the parameters of each attack function are randomly selected from a range of values. Some attackers may be aggressive in their attacks and they select small values for the parameters while other attackers may decide to select high values to launch stealthy attacks. The higher the value of the parameters, the more stealthy the attack, but the lower gains in terms of the amount of stolen energy. The details are as follows.

For function $f_1(\cdot)$, η is a random variable that is uniformly distributed over the interval $[0.3, 0.8]$ in which the lower η, the more profits the attacker can achieve. For function $f_3(\cdot)$, α_u is a random variable that is uniformly distributed over the interval $[3, 8]$. More reduction in the bill is achieved as α_u increases (i.e., Th_u increases). This is because the probability that the current consumption exceeds the upper limit decreases and, hence, the EU considers the last reported consumption r_l^i, which is lower than the current consumption r_c^i, to compute the bill. The range of α $[3, 8]$ increases the attacker's upper threshold Th_u between 40% and 90% in the case of 10% threshold, and between 20% and 45% in the case of 5% Threshold. Therefore, to be realistic, we consider different values for the attacker's threshold that can achieve enough gain to the attackers in terms of the reduction in the bill.

For functions $f_4(\cdot)$ and $f_5(\cdot)$, α_c and β_c are random variables that are uniformly distributed over the interval $[0.1, 0.6]$. The lower α_c and β_c, the more reduction in the bill the attacker can achieve. Hence, based on a data set of benign CAT readings from 114 customers over 349 days, the daily readings are considered a benign sample with a total of 39 786 (114 × 349) samples. Each sample contains 288 and 144 CAT readings for transmission rates of 1/5 and 1/10 min, respectively. Each sample is labeled 0 if it is benign, while it is labeled 1 if the sample is malicious. Then, the five proposed attacks are applied on each benign sample to create five malicious samples. After that, five balanced data sets, each data set corresponds to each attack, are created in which each data set has 79 572 equally distributed malicious and benign samples. Each data set is further divided into two parts, where 80% of the samples are used for training and 20% of the samples are used for evaluation. Next, we normalized both the training and evaluation data sets to transform the values of all features into a common range to make sure that no feature is dominating toward the detector's classification during the training. Moreover, normalizing the data helps the detector to speed up the training process which leads to faster convergence [32].

V. Benchmark Detectors

In this section, we discuss a set of shallow and deep-learning-based electricity-theft detectors for the CAT AMI using the reported consumption data, i.e., CAT readings. Two shallow and three deep learning classifiers are investigated in this article, where each detector is trained and evaluated using both benign and malicious data samples. These models will be used as benchmark detectors to compare their performance with our electricity-theft detector presented in Section VI. Moreover, we will use a combination of two deep learning models presented in this section (CNN and GRU) to build our electricity-theft detector.

1) *Shallow-Based Detectors:*

   RF-Based Detector (RF): This classifier builds a set of tree structures, where each tree consists of a set of branches and leaf nodes that represent a class label. RF is a well-known machine learning model that prevents overfitting while handling high-dimensional data and maintaining high computational efficiency [33]. RF uses ensemble learning, which is a technique that combines several classifiers to make accurate classifications.

   SVM-Based Detector (SVM): It is one of the widely used shallow classifiers in electricity-theft detection in the PT AMI. It separates different classes by constructing a hyperplane with the largest amount of margin [18]. The SVM-based electricity-theft detector is trained on both benign and malicious samples along with their labels in order to learn how to classify the sample's label during the evaluation stage [18].

2) *Deep-Learning-Based Detectors:*

   MLP-Based Detector: It is a well-known deep learning classifier which consists of: a) input layer which is the model's first layer where the input data is fed to; b) a set of hidden layers in which each layer has a number of neurons to process the output of the input layer; and c) output layer which is the last layer that outputs the classification result of the classifier [34]. Although MLP offers low computational complexity, it does not have the ability to exploit the temporal correlation in the electricity time-series consumption data.

   CNN-Based Detector: CNN detectors are widely used in solving machine learning problems, such as computer vision applications, natural language processing, and speech processing [35], which need a capability to extract the important features of the input data. A CNN model consists of input, convolution, fully connected, and output layers. The convolution layer composes of a group of filters and pooling layer(s). These filters are responsible for extracting the most important features from the given data by sliding each filter, which is usually small in size, over the input, while the pooling layer aims at reducing the data dimensionality on these extracted features while keeping the most important information. These operations are performed because the model performance becomes poor if the dimension of the data is large [35]. After the convolution layer(s), one or more fully connected feedforward layers are usually used to process the extracted features to be used by the output layer to compute the classification result. Moreover, a nonlinear activation function such as Tanh, ReLU, or Sigmoid is used after the convolution step to enable the model to make complex decisions and solve difficult tasks.

GRU-Based Detector: GRU is one type of recurrent neural networks which has a good ability to capture the sequential information and temporal correlation which exist in the customers' time-series readings [36]. This ability is due to the fact that GRU has the ability to remember long sequences of input patterns by the help of two gates, namely reset and update. These gates are responsible for controlling the flow of the information in order to learn the important information to retain. Moreover, GRU contains a set of hidden states in which each state acts as a memory. These states are used to hold/remember information on previous data as data is transferred from one layer to another; that is why, GRU can capture the correlations between the input data. The key component in GRU is the transition function in each time step t which takes the current time information X_t and the previous hidden state H_{t-1} and updates the current hidden state as follows:

$$H_t = F(X_t, H_{t-1}) \tag{1}$$

where F is a nonlinear transformation/activation function, e.g., Tanh and Sigmoid functions. Similarly, H_{t-1} considered the input at time $t-1$ and the state at time $t-2$ (H_{t-2}) and, thus, each state considers the previous states and inputs which enables the GRU to process a sequence of data.

VI. Electricity-Theft Detectors for CAT AMI

In this section, we first investigate adapting the CNN-GRU-based electricity-theft detector for the CAT AMI using the reported consumption data, i.e., CAT readings. Then, we discuss the rationale behind our electricity-theft detector's design. Finally, we will explain the architecture of the proposed detector in detail.

A. CNN-GRU-Based Detector

As mentioned earlier, the GRU-based detector can capture the temporal and complex correlation within the data. Instead of feeding the GRU model with a raw data, it can be fed with the important features of the input data to further improve the detection performance of the detector. Therefore, we investigate using a hybrid CNN and GRU model for electricity-theft detection for the CAT AMI. This architecture composes of 1-dimensional (1-D) convolutional and max-pooling layers followed by GRU layer(s). Hence, the 1-D convolutional and max-pooling layers act as a feature extractor and the GRU layer(s) further learn the temporal correlation within the extracted features of the CAT readings. An activation function is usually used to help the detector to make complex relationships between the input and output.

B. Rationale Behind Our Detector Design

Most of the recent studies about proposing electricity-theft detectors in the PT AMI have concluded that using machine learning-based detectors outperforms the state estimation-based and game-theory-based detectors in terms of the detector's accuracy [37]. While some of the machine learning-based electricity-theft detectors use shallow classifiers, such as SVM and RF, other detectors are based on deep learning architectures, such as RNN and CNN [23], [24].

Furthermore, these detectors are either general, which can be used for all customers, or customized (i.e., customer specific) which is used for only one customer. The problem of the customized detectors is that they cannot be used to detect new malicious customers until there is enough consumption data of that customer for the training process. Moreover, they are vulnerable to data contamination attacks where malicious customers report false readings during the training process to avoid being detected during the evaluation [37]. On the other hand, general detectors are more robust against such attacks since they are trained on the data of a large number of customers, and, thus, new malicious customers can be detected. Also, customer-specific detectors need a lot of computation resources because too many detectors should be trained, i.e., one detector should be trained for each customer.

In addition, since the transmission pattern may change when a customer reports false readings, the detector's ability to learn the correlations between the CAT readings and the transmission pattern is important. Moreover, the transmission pattern contains information about the customer's behavior that can help the electricity-theft detector to make accurate classifications. Therefore, we take the transmission pattern into consideration as a second input to the detector in addition to the CAT readings, as can be seen in Fig. 5, to further help the detector in identifying electricity theft.

According to the preceding discussion, our detector shall: (1) be general which can be used for any customer including the new ones by training it using the data collected from all customers; (2) consider the transmission pattern as well as the CAT readings to boost the performance of the detector instead of depending only on the SMs' CAT readings for the design of the electricity-theft detector; and (3) capture the correlation within the CAT readings and the relation between the CAT readings and the transmission pattern by using a deep learning architecture and, thus, the detector shall be able to make accurate classifications.

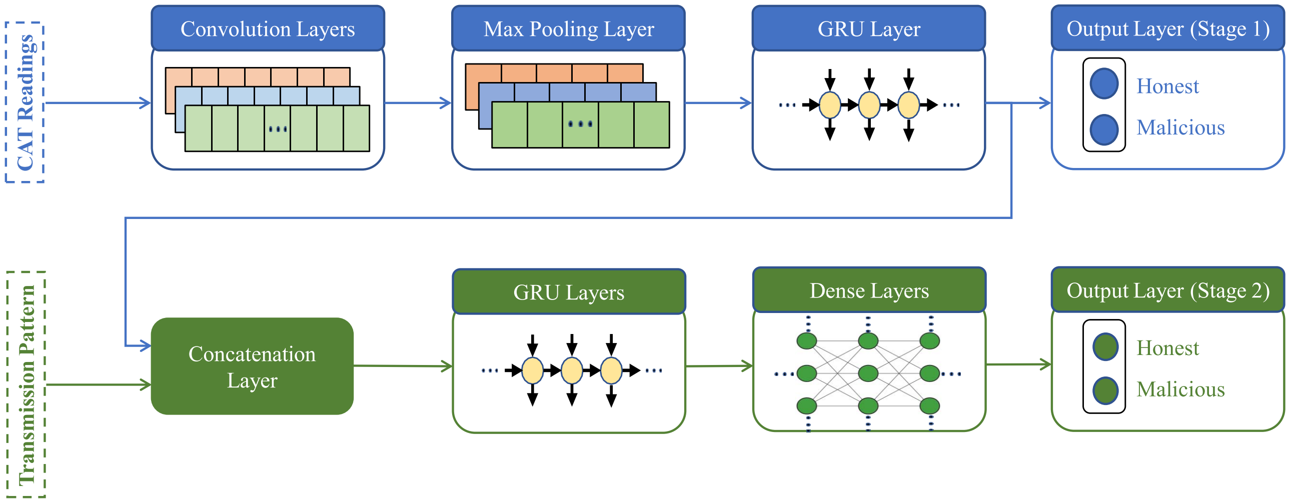


Fig. 5. Architecture of our electricity-theft cyberattack detector for CAT AMI.

C. Architecture of Our Detector

Our detector takes two inputs in parallel; the first input is the CAT readings of one day, while the second input is the transmission pattern of the same day. These two inputs lead to designing a two-stage detector, as shown in Fig. 5, to boost the detector's performance in detecting malicious customers. These stages are described as follows.

1) The first stage of our detector processes solely one type of input data, which is the CAT readings. This stage is a hybrid deep-learning model that contains a CNN with GRU neural networks. We use 1-D CNN neural network (1-D CNN) because of its ability to capture and extract the important features of the 1-D time-series CAT readings and, hence, this results in a high detection performance. Furthermore, we use the GRU architecture to capture the time correlations of the consecutive CAT readings.
2) The second stage of our detector takes the transmission pattern as an input and concatenates it with the output of the first stage. In this stage, a set of GRU layers is used to enhance the detector's capability in capturing the correlation between the CAT readings and the corresponding transmission pattern. Moreover, these GRU layers are followed by a fully connected neural network to be able to make accurate classifications.

In order to evaluate the impact of processing the transmission pattern on the detection performance, we first evaluate our detector without the transmission pattern, i.e., the output of the first stage of the detector. Then, we evaluate our detector's performance after considering the transmission pattern, i.e., the output of the second stage of our detector, as shown in Fig. 5.

VII. Evaluations

This section first presents our experimental environment and the metrics that we use to evaluate our detector's performance. Then, we evaluate our electricity-theft detector's performance by conducting two experiments. The first experiment investigates different machine learning models to detect malicious customers who launch electricity-theft cyberattacks using only the CAT readings reported by SMs. On the other hand, the second experiment investigates the improvement in the detector's performance when considering the transmission pattern of the SMs in addition to the reported CAT readings.

A. Experimental Setup

In this work, all experiments are conducted with the high-performance cluster (HPC) of the Tennessee Tech University using one NVIDIA Tesla K80 GPU. During the learning stage of our detectors, we used a hyperopt tool [38] on a validation data set to appropriately fine-tune the detectors' hyperparameters, e.g., number of units per layer, activation function for each layer, etc. Moreover, *Adam* optimizer [39] is used to train our detectors for 200 epochs, 0.001 learning rate, 256 batch size, and categorical cross entropy as the loss function. Also, we used various Python3 libraries in our experiments as follows. Numpy is used to prepare our data set, while Keras [40] and Scikit-learn [41] are used to train and evaluate our detectors, respectively. Moreover, Matplotlib [42] is used for data visualization.

B. Evaluation Metrics

Since electricity-theft detection is a binary classification problem, we denote the malicious samples as the positive class and benign samples as the negative class. Given that true positive (TP) is the number of samples that are correctly classified as malicious, true negative (TN) is the number of samples that are correctly classified as honest, false positive (FP) is the number of honest samples that are misclassified as malicious, and false negative (FN) is the number of malicious samples that are misclassified as honest, the performance of our detector is assessed by using a set of evaluation metrics as follows.

1) *Accuracy (ACC):* It measures the percentage of the honest/malicious samples that are classified as

TABLE III

COMPARISON BETWEEN THE PERFORMANCE OF DIFFERENT BENCHMARK MACHINE LEARNING-BASED ELECTRICITY-THEFT DETECTORS AT 1/5-MIN TRANSMISSION RATE AND 10% THRESHOLD. (A) PERFORMANCE OF DIFFERENT TYPES OF SHALLOW-BASED DETECTORS. (B) PERFORMANCE OF DIFFERENT TYPES OF DEEP-LEARNING-BASED DETECTORS

(a)

Attacks	**SVM**				**RF**			
	ACC (%)	**DR** (%)	**FA** (%)	**HD** (%)	**ACC** (%)	**DR** (%)	**FA** (%)	**HD** (%)
Attack 1	85.9	87.35	17.1	70.25	84.8	85.67	14.92	70.75
Attack 2	83.43	89.34	17.98	71.36	80.92	85.54	23.7	61.84
Attack 3	85	92.47	23.5	68.92	91.13	88.95	6.64	82.3
Attack 4	88	95	19	76	93.3	90.82	4.2	86.62
Attack 5	88.84	97.55	19.74	77.8	95.56	96.07	15.8	80.27

(b)

Attacks	**MLP**				**CNN**				**GRU**			
	ACC (%)	**DR** (%)	**FA** (%)	**HD** (%)	**ACC** (%)	**DR** (%)	**FA** (%)	**HD** (%)	**ACC** (%)	**DR** (%)	**FA** (%)	**HD** (%)
Attack 1	86.15	90.02	17.71	72.31	90.84	91.59	9.9	81.68	**91.52**	**90.57**	**7.52**	**83.05**
Attack 2	83.15	93.68	27.38	66.3	92.86	95.14	9.43	85.72	**93.17**	**97.16**	**10.81**	**86.35**
Attack 3	93.43	96.65	9.83	86.82	**96.16**	**97.47**	**5.16**	**92.3**	96.02	97	4.96	92.04
Attack 4	93.52	97.46	10.44	87.02	**96.88**	**98.62**	**4.85**	**93.77**	96.82	98.8	5.13	93.67
Attack 5	90.49	92.1	11.08	81.01	**96.36**	**97.43**	**4.71**	**92.72**	96.19	97.14	4.76	92.38

honest/malicious. It is computed by using the following expression:

$$\mathrm{ACC}(\%) = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \times 100.$$

2) *Detection Rate (DR):* It measures the percentage of the malicious samples that are classified as malicious with respect to the total actual number of malicious samples in the data set. It is computed by using the following expression:

$$\mathrm{DR}(\%) = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \times 100.$$

3) *False Alarm (FA):* It measures the percentage of the honest samples that are misclassified as malicious with respect to the total number of honest samples in the data set. It is computed by using the following expression:

$$\mathrm{FA}(\%) = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \times 100.$$

4) *Highest Difference (HD):* It is the difference between DR and FA

$$\mathrm{HD}(\%) = \mathrm{DR}(\%) - \mathrm{FA}(\%).$$

5) *Receiver Operating Characteristic (ROC) Curve:* It is usually used to assess the performance of a classifier which is determined by the area under the ROC curve (AUC) [43]. The higher this area, the better the classifier performance in identifying the classes.

The detector's performance is better when DR, HD, and ACC are high, and FA is low.

C. Results of Experiment 1

To demonstrate the effectiveness of the proposed electricity-theft detector, we first compare the performance of different benchmark shallow-based and deep-learning-based detectors by considering only the CAT readings reported by the customers' SMs for three use cases; 1/10-min transmission rate at 5% and 10% thresholds and 1/5-min transmission rate at 10% threshold. The benchmark shallow detectors are SVM and RF, while the benchmark deep learning detectors are MLP, CNN, and GRU.

In this experiment, to ensure a fair performance comparison, we used the data set that is discussed in Section IV to train and evaluate the detectors discussed in Section V. We train our detectors, where each detector can identify one attack, using both honest and malicious samples. The performance of the detectors is evaluated using the five different attacks discussed in Section IV-B, separately. We randomly chose 20% of the samples in our data set for evaluation and 80% of the samples for training the detectors.

Results and Discussion: Tables III–V present the performance of different types of machine learning-based electricity-theft detectors including shallow and deep learning architectures for the three use cases, where subtable (a) presents the performance of benchmark shallow-based detectors and subtable (b) presents the performance of benchmark deep-learning-based detectors. The performance of the detectors is evaluated using the following metrics; HD, DR, FA, and ACC. First, it can be seen from the given results that both MLP and shallow-based detectors achieve the lowest performance in identifying the five electricity-theft

TABLE IV

COMPARISON BETWEEN THE PERFORMANCE OF DIFFERENT BENCHMARK MACHINE LEARNING-BASED ELECTRICITY-THEFT DETECTORS AT 1/10-MIN TRANSMISSION RATE AND 10% THRESHOLD. (A) PERFORMANCE OF DIFFERENT TYPES OF SHALLOW-BASED DETECTORS. (B) PERFORMANCE OF DIFFERENT TYPES OF DEEP-LEARNING-BASED DETECTORS

(a)

Attacks	SVM				RF			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	80.55	89.26	18.1	71.61	86.23	85.2	20.56	64.64
Attack 2	79.62	85.74	26.52	59.23	84.45	86.23	17.33	68.9
Attack 3	84.88	90.57	20.97	69.6	88.62	86.8	9.51	77.29
Attack 4	86.3	92.21	19.16	72.69	90.01	88.02	8.04	79.98
Attack 5	85.9	93.56	21.55	72.01	93.16	94.58	14.38	80.2

(b)

Attacks	MLP				CNN				GRU			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	84.48	89.14	18.92	80.22	92.47	91.38	6.43	84.95	**93.48**	**93.2**	**6.24**	**86.96**
Attack 2	82.54	88.78	23.7	65.07	**93.44**	**94.66**	**7.78**	**86.88**	93.28	94.44	7.88	86.56
Attack 3	86.91	89.53	15.79	73.74	93.2	92.84	6.43	86.4	**94.55**	**95.09**	**6.01**	**89.08**
Attack 4	89.18	89.98	11.59	78.38	96.77	98.42	4.83	93.59	**96.76**	**98.76**	**5.16**	**93.6**
Attack 5	89.18	91.71	13.27	78.44	96.02	97.06	5	92.06	**96.48**	**97.79**	**4.8**	**92.99**

TABLE V

COMPARISON BETWEEN THE PERFORMANCE OF DIFFERENT BENCHMARK MACHINE LEARNING-BASED ELECTRICITY-THEFT DETECTORS AT 1/10-MIN TRANSMISSION RATE AND 5% THRESHOLD. (A) PERFORMANCE OF DIFFERENT TYPES OF SHALLOW-BASED DETECTORS. (B) PERFORMANCE OF DIFFERENT TYPES OF DEEP-LEARNING-BASED DETECTORS

(a)

Attacks	SVM				RF			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	83.39	89.13	22.52	66.62	89.68	88.64	9.26	79.38
Attack 2	77.6	83.76	28.74	55.03	82.17	84.97	20.7	64.27
Attack 3	92.48	86.1	14.64	71.46	92.38	92.16	7.39	84.77
Attack 4	87.14	92.81	18.68	74.13	93.41	94.79	8.02	86.78
Attack 5	86.4	94.15	21.55	72.59	90.68	88.1	6.67	81.42

(b)

Attacks	MLP				CNN				GRU			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	85.74	89.45	18.07	71.38	92.23	93.17	8.75	84.42	**92.83**	**93.58**	**7.95**	**85.64**
Attack 2	81.25	82.51	20.04	64.47	**94.09**	**95.67**	**7.54**	**88.13**	94.05	93.55	5.43	88.12
Attack 3	83.47	84.54	17.63	66.91	96.08	98.41	6.32	92.09	**96.1**	**98.58**	**6.45**	**92.12**
Attack 4	89.04	89.96	11.91	78.06	**96.42**	**97.6**	**4.79**	**92.81**	96.41	98.31	5.54	92.78
Attack 5	89.33	90.92	12.31	78.61	95.49	96.54	5.59	90.96	**96.24**	**97.07**	**4.62**	**92.45**

cyberattacks. Second, we can see that both the GRU and CNN-based detectors provide a better performance compared to the MLP and shallow-based detectors because GRU has a good ability to capture the temporal correlation between the consecutive CAT readings while the CNN-based detector has the ability of extracting the important features of the CAT readings using a set of filters, which can enhance the detector's performance. Our goal from this experiment is to

TABLE VI
OPTIMAL HYPERPARAMETERS OF OUR TWO-STAGE DETECTOR FOR ATTACK 1 AT 1/10-MIN TRANSMISSION RATE AND 5% THRESHOLD

Stage	Hyper-parameters		
	Layer	**Number of units**	**AF**
Stage 1	Input	144	Linear
	Conv1D	128	Tanh
	Conv1D	256	Relu
	MaxPooling1D	2	–
	GRU	128	Relu
	Output	2	Softmax
Stage 2	Input	144	Linear
	GRU	128	Sigmoid
	GRU	128	Relu
	Dense	64	Tanh
	Dense	512	Tanh
	Dense	64	Relu
	Output	2	Softmax

determine the best performing benchmark detector for each attack and we highlight it in bold font based on the value of HD, as shown in Tables III–V.

D. Results of Experiment 2

This section compares the performance of the proposed two electricity-theft detectors (the output of Stages 1 and 2) with the best performing benchmark detectors evaluated in experiment 1 as shown in Fig. 5 to assess the benefit of having a hybrid detector and taking the transmission pattern into consideration. The data set discussed in Section IV is used to train our detector as follows. Only the CAT readings are used for training Stage 1, while the transmission pattern in addition to the CAT readings are used for training Stage 2. As mentioned earlier, we used Hyperopt to optimize the detectors' hyperparameters. For instance, our two-stage detector's optimal hyperparameters for Attack 1 at 1/10-min transmission rate and 5% threshold can be seen in Table VI.

Results and Discussion: Table VII presents the values of ACC, DR, FA, and HD of the best performing benchmark detectors evaluated in experiment 1, our hybrid CNN-GRU detector trained on the CAT readings only (Stage 1), and the proposed two-stage detector trained on both CAT readings and transmission pattern (Stage 2) in identifying the five cyberattacks at different transmission rates and thresholds. Furthermore, Fig. 6 shows the difference in the performance between the CNN-GRU-based detector that processes CAT readings only and our two-stage detector that processes transmission pattern in addition to CAT readings using ROC curves for Attack 2 at 1/5-min transmission rate and 10% threshold. It can be seen that among all the best benchmark detectors, CNN-GRU-based detectors provide the highest performance because the combination of CNN and GRU can extract the important features from the input CAT readings and capture the correlation between the extracted features, which is the key to improve the detector's performance. Moreover, we can see from the results that the performance of the detectors is not affected by the values of the transmission rates and thresholds. Hence, the hybrid CNN-GRU architecture is selected for designing the proposed electricity-theft detector.

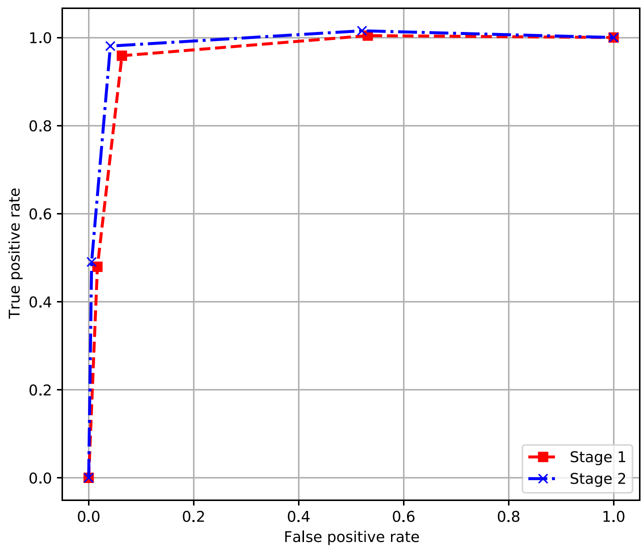


Fig. 6. Comparison between the ROC curves of Stages 1 and 2 for Attack 2 at 1/5-min transmission rate and 10% threshold.

It can be seen from the results of the experiment that our two-stage detector outperforms the other detectors in detecting all the attacks. The superiority of our detector (Stage 2) over the detectors that process only the CAT readings (Stage 1) is because it considers additional important features, i.e., transmission pattern, which helps the detector to make a more accurate classification boundary between the malicious and benign samples. Moreover, our detector captures the correlations between the CAT readings and the corresponding transmission pattern. So, if a malicious customer tampers with his SM's readings, this may have an impact on the correlations between the CAT readings and the transmission pattern. This means that having additional features allows our detector to differentiate between the malicious and benign samples by checking the correlations between the CAT readings and the transmission pattern. This enhances the detector's performance, i.e., higher DR, lower FA and, hence, higher HD, as can be seen in Table VI. Finally, considering transmission patterns increases the HD by about 1% to 4% comparing to the HD obtained by using only the CAT readings as can be observed from Table VI.

On the other hand, it can be observed that Attacks 1 and 2 are the most difficult to detect comparing to the other attacks. This can be explained by the fact that Attack 1 makes the transmission patterns of the reported readings similar to the patterns of the true readings to confuse the detector and also makes the malicious consumption pattern look like the real pattern but with lower magnitudes to reduce his/her bill. On the other hand, Attack 2 confuses the electricity-theft detector by reporting some true readings (when $r_c^i < x_l^i$), which makes it hard for the detector to detect. Despite the stealthiness of the proposed attacks, the given results demonstrate that our detector shows good performance under different cyberattacks at different transmission rates and thresholds.

TABLE VII

COMPARISON BETWEEN THE PERFORMANCE OF THE BEST BENCHMARK ELECTRICITY-THEFT DETECTOR, CNN-GRU (STAGE 1), AND TWO-STAGE DETECTOR (STAGE 2) AT DIFFERENT TRANSMISSION RATES AND THRESHOLDS. (A) 1/5-MIN TRANSMISSION RATE AT 10% THRESHOLD. (B) 1/10-MIN TRANSMISSION RATE AT 10% THRESHOLD. (C) 1/10-MIN TRANSMISSION RATE AT 5% THRESHOLD

(a)

Attacks	Best performing benchmark detector				CNN-GRU (Stage 1)				Our two-stage detector (Stage 2)			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	91.52	90.57	7.52	83.05	93.42	93	6.16	86.84	**95.25**	**94.31**	**3.81**	**90.5**
Attack 2	93.17	97.16	10.81	86.35	94.45	95.38	6.48	88.81	**95.56**	**95.29**	**4.16**	**91.13**
Attack 3	96.16	97.47	5.16	92.3	96.78	97.4	3.84	93.55	**97.66**	**97.82**	**2.5**	**95.32**
Attack 4	96.88	98.62	4.85	93.77	98.37	99.39	2.65	96.75	**98.96**	**99.07**	**1.14**	**97.92**
Attack 5	96.36	97.43	4.71	92.72	97.22	97.79	3.36	94.43	**98.28**	**98.42**	**1.86**	**96.55**

(b)

Attacks	Best performing benchmark detector				CNN-GRU (Stage 1)				Our two-stage detector (Stage 2)			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	93.48	93.2	6.24	86.96	93.77	95.74	8.23	87.51	**95.39**	**92.49**	**1.66**	**90.83**
Attack 2	93.44	94.66	7.78	86.88	95.1	96.35	6.15	90.2	**95.61**	**94.4**	**3.15**	**91.25**
Attack 3	94.55	95.09	6.01	89.08	95.54	95.83	4.75	91.08	**96.85**	**97.22**	**3.53**	**93.69**
Attack 4	96.76	98.76	5.16	93.6	96.98	98.42	4.43	93.99	**97.81**	**98.17**	**2.56**	**95.61**
Attack 5	96.48	97.79	4.8	92.99	96.84	97.53	3.84	93.69	**97.7**	**99.45**	**4.08**	**95.37**

(c)

Attacks	Best performing benchmark detector				CNN-GRU (Stage 1)				Our two-stage detector (Stage 2)			
	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)	ACC (%)	DR (%)	FA (%)	HD (%)
Attack 1	92.83	93.58	7.95	85.64	93.98	94.42	5.43	87.98	**94.85**	**94.82**	**5.11**	**89.71**
Attack 2	94.09	95.67	7.54	88.13	94.66	95.87	6.57	89.29	**95.79**	**97.48**	**5.94**	**91.55**
Attack 3	96.1	98.58	6.45	92.12	96.86	97.6	3.91	93.7	**97.21**	**96.36**	**1.93**	**94.44**
Attack 4	96.42	97.6	4.79	92.81	97.24	97.64	3.18	94.46	**97.74**	**97.72**	**2.24**	**95.48**
Attack 5	96.24	97.07	4.62	92.45	96.79	97.44	3.87	93.56	**97.43**	**98**	**3.15**	**94.85**

VIII. CONCLUSION

In this article, we have investigated detecting electricity-theft cyberattacks in the CAT AMI network. Specifically, we have processed a real power consumption readings data set to create a benign data set for the CAT approach and proposed a new set of cyberattacks to create malicious samples. Then, we developed a deep-learning-based electricity-theft detection solution to identify malicious customers for the CAT AMI network. Our detector has been trained on the customers' transmission patterns and CAT readings to learn the correlation between them. Extensive experiments have been conducted, and the results indicated that our detector can accurately identify malicious customers. Furthermore, the results showed that our multi-input detector achieves higher DR and lower FA than a single-input detector trained only on the CAT readings. Although reporting the customers' CAT readings enables the EU to detect malicious customers, revealing these readings to the EU endangers the customers' privacy. This is because the readings can leak private information about customers' lifestyle, e.g., the appliances being used, presence/absence of the customers, etc. To preserve customers' privacy, the SMs' readings should be encrypted and sent to the EU. However, in this case, it would be difficult for the EU to make sure that the customers follow the CAT approach and, hence, attackers can launch new attacks which are not considered in this article. Therefore, we will investigate, in our future work, this privacy issue for the CAT AMI network.

ACKNOWLEDGMENT

The authors, therefore, acknowledge with thanks to DSR for technical and financial support.

REFERENCES

[1] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[2] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[3] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.

[4] M. I. Ibrahem, M. M. Badr, M. M. Fouda, M. Mahmoud, W. Alasmary, and Z. M. Fadlullah, "PMBFE: Efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks," in *Proc. IEEE Int. Symp. Netw. Comput. Commun. (ISNCC)*, Montreal, QC, Canada, Oct. 2020, pp. 1–7.

[5] M. I. Ibrahem, M. Nabil, M. M. Fouda, M. E. A. Mahmoud, W. Alasmary, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1243–1258, Jan. 2021.

[6] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security Privacy*, vol. 8, no. 1, pp. 11–20, Jan./Feb. 2010.

[7] K. Samarakoon, J. Ekanayake, and N. Jenkins, "Reporting available demand response," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1842–1851, Dec. 2013.

[8] K. C. Armel, A. Gupta, G. Shrimali, and A. Albert, "Is disaggregation the holy grail of energy efficiency? The case of electricity," *Energy Policy*, vol. 52, pp. 213–234, Jan. 2013.

[9] S. Werner and J. Lunden, "Event-triggered real-time metering in smart grids," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2015, pp. 2701–2705.

[10] S. Werner and J. Lundén, "Smart load tracking and reporting for real-time metering in electric power grids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1723–1731, May 2016.

[11] J. Lunden and S. Werner, "Real-time smart metering with reduced communication and bounded error," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2014, pp. 326–331.

[12] M. Simonov, G. Chicco, and G. Zanetto, "Event-driven energy metering: Principles and applications," *IEEE Trans. Ind. Appl.*, vol. 53, no. 4, pp. 3217–3227, Jul./Aug. 2017.

[13] H. Li, S. Gong, L. Lai, Z. Han, R. C. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1540–1551, Sep. 2012.

[14] M. I. Ibrahem, M. M. Badr, M. Mahmoud, M. M. Fouda, and W. Alasmary, "Countering presence privacy attack in efficient AMI networks using interactive deep-learning," in *Proc. IEEE Int. Symp. Netw. Comput. Commun. (ISNCC)*, Dubai, UAE, Nov. 2021, pp. 1–7.

[15] M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, W. Alasmary, and X. Shen, "Privacy preserving and efficient data collection scheme for AMI networks using deep learning," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 17131–17146, Dec. 2021, doi: 10.1109/JIOT.2021.3077897.

[16] A. Alsharif, M. Nabil, M. Mahmoud, and M. Abdallah, "Privacy-preserving collection of power consumption data for enhanced AMI networks," in *Proc. Int. Conf. Telecommun. (ICT)*, Jun. 2018, pp. 196–201.

[17] "Electricity thefts surge in bad times." Accessed: Mar. 2020. [Online]. Available: https://www.usatoday30.usatoday.com/money/industries/energy/2009-03-16-electricity-thefts_N.htm

[18] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[19] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jul. 2019.

[20] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[21] V. Ford, A. Siraj, and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," in *Proc. IEEE Symp. Comput. Intell. Appl. Smart Grid (CIASG)*, 2014, pp. 1–6.

[22] M. M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Detection of non-technical losses using smart meter data and supervised learning," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2661–2670, May 2019.

[23] R. R. Bhat, R. D. Trevizan, R. Sengupta, X. Li, and A. Bretas, "Identifying nontechnical power loss via spatial and temporal deep learning," in *Proc. IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, 2016, pp. 272–279.

[24] M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero, and A. Gómez-Expósito, "Hybrid deep neural networks for detection of non-technical losses in electricity smart meters," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1254–1263, Mar. 2020.

[25] "Residential energy disaggregation dataset (REDD)." Kolter. Accessed: 2020. [Online]. Available: http://traces.cs.umass.edu/index.php/Smart/Smart

[26] Z. Yan and H. Wen, "Electricity theft detection base on extreme gradient boosting in AMI," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–9, Jan. 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9312127

[27] "Irish social science data archive." Accessed: Sep. 2020. [Online]. Available: https://www.ucd.i.e.,/issda/data/commissionforenergyregulationcer/

[28] "State grid corporation of China." Accessed: Sep. 2020. [Online]. Available: http://www.sgcc.com.cn/

[29] M. M. Badr, M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmary, "Detection of false-reading attacks in smart grid net-metering system," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1386–1401, Jan. 2022, doi: 10.1109/JIOT.2021.3087580.

[30] V. B. Krishna, C. A. Gunter, and W. H. Sanders, "Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 790–805, Aug. 2018.

[31] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2019.

[32] "Feature scaling and normalisation in a nutshell." Accessed: Sep. 2020. [Online]. Available: https://medium.com/analytics-vidhya/feature-scaling-and-normalisation-in-a-nutshell-5319af86f89b

[33] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity theft detection in power grids with deep learning and random forests," *J. Elect. Comput. Eng.*, vol. 2019, Oct. 2019, Art. no. 4136874. [Online]. Available: https://www.hindawi.com/journals/jece/2019/4136874/

[34] S. Haykin, *Neural Networks and Learning Machines: A Comprehensive Foundation*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, Nov. 2008.

[35] Y. LeCun and Y. Bengio, "Convolutional networks for images, speech, and time series," in *The Handbook of Brain Theory and Neural Networks*, M. Arbib, Ed. Cambridge, MA, USA: MIT Press, 1995, pp. 255–258.

[36] D. Lavrova, D. Zegzhda, and A. Yarmak, "Using GRU neural network for cyber-attack detection in automated process control systems," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Jun. 2019, pp. 1–3.

[37] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Serpedin, "Deep recurrent electricity theft detection in AMI networks with random tuning of hyper-parameters," in *Proc. Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 740–745.

[38] J. Bergstra, B. Komer, C. Eliasmith, D. Yamins, and D. D. Cox, "Hyperopt: A python library for model selection and hyperparameter optimization," *Comput. Sci. Discov.*, vol. 8, no. 1, 2015, Art. no. 14008. [Online]. Available: https://doi.org/10.1088/1749-4699/8/1/014008

[39] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proc. Int. Conf. Learn. Represent.*, San Diego, CA, USA, May 2015, pp. 1–14.

[40] F. Chollet *et al.* "Keras." 2015. [Online]. Available: https://github.com/fchollet/keras

[41] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Oct. 2011.

[42] J. D. Hunter, "Matplotlib: A 2D graphics environment," *Comput. Sci. Eng.*, vol. 9, no. 3, pp. 90–95, May/Jun. 2007.

[43] A. P. Bradley, "The use of the area under the ROC curve in the evaluation of machine learning algorithms," *Pattern Recognit.*, vol. 30, no. 7, pp. 1145–1159, Jul. 1997.

Mohamed I. Ibrahem received the B.S. degree in electrical engineering and M.S. degree in electronics and communications from Benha University, Cairo, Egypt, in 2014 and 2018, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, Cookeville, TN, USA, in 2021.

He is currently an Assistant Professor with the Department of Cyber Security Engineering, George Mason University, Fairfax, VA, USA. He is also holding the position of a Lecturer Assistant with the Faculty of Engineering at Shoubra, Benha University. His research interests include machine learning, cryptography and network security, and privacy-preserving schemes for smart grid communication, and AMI networks.

Dr. Ibrahem received the Eminence Award for the Doctor of Philosophy Best Paper from Tennessee Tech University.

Mohamed M. E. A. Mahmoud (Senior Member, IEEE) received the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in April 2011.

He worked as a Postdoctoral Fellow with the Broadband Communications Research Group, University of Waterloo from May 2011 to May 2012. From August 2012 to July 2013, he worked as a Visiting Scholar with the University of Waterloo, and a Postdoctoral Fellow with Ryerson University, Toronto, ON, Canada. He is currently an Associate Professor with the Department Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN, USA. He has authored more than 23 papers published in major IEEE conferences and journals, such as INFOCOM Conference and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. His research interests include security and privacy preserving schemes for smart grid communication network, mobile ad hoc network, sensor network, and delay-tolerant network.

Dr. Mahmoud has received the NSERC-PDF Award. He won the Best Paper Award from IEEE International Conference on Communications (ICC'09), Dresden, Germany, in 2009. He serves as an Associate Editor for the *Peer-to-Peer Networking and Applications* (Springer). He served as a Technical Program Committee Member for several IEEE conferences and as a Reviewer for several journals and conferences, such as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and *Peer-to-Peer Networking*.

Fawaz Alsolami (Member, IEEE) received the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008, and the Ph.D. degree in computer science from KAUST University, Thuwal, Saudi Arabia, in 2016.

He joined the Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia, as an Assistant Professor of Computer Science, after which he held an Associate Professor position. He also published many articles and one monograph. His research interests are artificial intelligence, machine learning and data mining, and combinatorial optimization.

Waleed Alasmary (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer engineering from Umm Al-Qura University, Mecca, Saudi Arabia, in 2005, the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2010, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2015.

During his Ph.D. degree, he was a Visiting Research Scholar with the Network Research Laboratory, University of California at Los Angeles, Los Angeles, CA, USA, in 2014. He was a Fulbright Visiting Scholar with the CSAIL Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA, from 2016 to 2017. He subsequently joined the College of Computer and Information Systems, Umm Al-Qura University, as an Assistant Professor of Computer Engineering, after which he held an Associate Professor position. From 2020 to 2022, he was the IT and Emerging Technology Advisor for the Governor of the Communication and Information Technology Commission, Riyadh, Saudi Arabia, where he has been the Founding Director of the Research and Innovation Center since 2021. He has more than 60 research papers in prestigious conferences and journals, and four U.S. Patents. His current research interests are in emerging topics, including blockchain and privacy-preserving systems, and machine learning in smart systems.

Abdullah Saad AL-Malaise AL-Ghamdi received the Ph.D. degree in computer science from George Washington University, Washington, DC, USA, in 2003.

He is a Professor of Software and Systems Engineering and AI, and associated with the Information Systems (IS) Department, Faculty of Computing and Information Technology (FCIT), King Abdulaziz University (KAU), Jeddah, Saudi Arabia, where he is currently working as a Head of Consultant's Unit and the Computer Skills Department, FCIT, and the Vice-President of the Development Office. He is also performing his task as a Consultant to Vice-President for the Graduate Studies and Scientific Research, KAU. He has previously worked as the Head of the IS Department, and the Vice Dean of the Graduate Studies and Scientific Research, FCIT. In addition to teaching several courses to master's and Ph.D. students, he is actively supervising many postgraduate internal and external student's thesis. He has been a part of different evaluation processes, such as Curriculum Evaluation, Promotion Evaluation, and Research Proposal Evaluation. He is an active member of the KAU Scientific Council, Deanship of Graduate Studies Council, and Scholarship and Training Committee. He has published two books and more than 70 research articles in well-known venues, such as the Web of Science, Springer, IEEE, and Taylor & Francis. The current researches under development include AI in digital education, machine learning approach on Corona disease, and cognitive assessment on medical data. His areas of research and interests are software engineering and systems, artificial intelligence, data analytics, business intelligence, IT-business-oriented architecture, business process re-engineering, data mining, and decision support system.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990.

He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks.

Dr. Shen received the R.A. Fessenden Award in 2019 from IEEE, Canada, the Award of Merit from the Federation of Chinese Canadian Professionals (Ontario) presents in 2019, the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, the Joseph LoCicero Award in 2015, the Education Award in 2017 from the IEEE Communications Society, the Technical Recognition Award from Wireless Communications Technical Committee in 2019 and AHSN Technical Committee in 2013, and also the Excellent Graduate Supervision Award in 2006 from the University of Waterloo and the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada. He served as the Technical Program Committee Chair/Co-Chair for the IEEE Globecom'16, IEEE Infocom'14, IEEE VTC'10 Fall, and IEEE Globecom'07, the Symposia Chair for the IEEE ICC'10, and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications. He is the Elected IEEE Communications Society Vice President for Technical and Educational Activities, the Vice President for Publications, the Member-at-Large on the Board of Governors, the Chair of the Distinguished Lecturer Selection Committee, and the Member of the IEEE Fellow Selection Committee. He was/is the Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, *IET Communications*, and *Peer-to-Peer Networking and Applications*. He is a registered Professional Engineer of Ontario, Canada, a Fellow of the Engineering Institute of Canada, Canadian Academy of Engineering, and Royal Society of Canada, a Foreign Fellow of the Chinese Academy of Engineering, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society.