IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 June 2023, accepted 23 June 2023, date of publication 30 June 2023, date of current version 12 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3291217

RESEARCH ARTICLE

Privacy-Preserving Detection of Power Theft in Smart Grid Change and Transmit (CAT) Advanced Metering Infrastructure

MOHAMMED J. ABDULAAL[1,2], MOHAMED M. E. A. MAHMOUD[3,4], (Senior Member, IEEE), SAHEED A. BELLO[1], JUNAID KHALID[1], ABDULAH JEZA ALJOHANI[1,2], AHMAD H. MILYANI[1], ABDULLAH M. ABUSORRAH[1], (Senior Member, IEEE), AND MOHAMED I. IBRAHEM[5,6]

[1]Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]Center of Excellence in Intelligent Engineering Systems (CEIES), King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Department of Electrical and Computer Engineering, Tennessee Technological University, Cookeville, TN 38505, USA
[4]KINDI Center for Computing Research, Qatar University, Doha, Qatar
[5]School of Computer and Cyber Sciences, Augusta University, Augusta, GA 30912, USA
[6]Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11672, Egypt

Corresponding author: Mohamed M. E. A. Mahmoud (mmahmoud@tntech.edu)

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number IFPRC-093-135-2020 and King Abdulaziz University, Deanship of Scientific Research (DSR), Jeddah, Saudi Arabia.

ABSTRACT For energy management and billing purposes, advanced metering infrastructure (AMI) requires periodic transmission of consumer power consumption readings by smart meters to the electric utility (EU). An efficient way for collecting readings is the change-and-transmit approach (CAT AMI) whereby readings are only transmitted if there is an enough change in consumption readings. CAT AMI, however, is plagued by malicious consumers who hack their smart meters to illegally lower their electricity bills by falsifying their readings. These attacks on the AMI could have bad economic consequences and impair the performance of the power grid if these readings are used for managing the grids. Machine learning models can be used to detect false readings but this requires disclosing consumers' CAT readings to the EU to evalaute the model. However, disclosing the consumers' readings jeopardizes consumers' privacy due to the fact that these readings can reveal sensitive information about consumers' lifestyles, e.g., their presence or absence, the appliances they use, etc. The problems of detecting power theft while protecting the consumers' privacy in CAT AMI is investigated in this paper. First, a dataset of actual readings to generate a benign dataset is developped followed by proposing new cyber-attacks tailored for CAT AMI to generate malicious samples. Then, two deep-learning detectors using a baseline model (CNN) and a CNN-GRU model are trained to detect power thefts in CAT AMI. To preserve consumers' privacy, the paper develops an approach to enable the EU to evaluate the detector using encrypted data without being able to learn the readings. Extensive experiments were carried out to assess our proposal, and the results indicate that our proposal is capable of accurately identifying malicious consumers with acceptable overhead while preserving the privacy of the consumers. Specifically, comparing to CNN model, our CNN-GRU model increases the detection rate from 93.85% to 97.14% and *HD* from to 87.7% to 94.28%, respectively.

INDEX TERMS Privacy preservation, security, detection of false readings, power theft, AMI networks, smart grid.

I. INTRODUCTION

A smart grid offers great improvement to the traditional power grid as many countries of the world increasingly embrace this technology. Smart grids provide a reduction in the emission of greenhouse gases, increased reliability in the delivery of electricity and optimized grid operation [1], [2], [3]. Smart grids consist of advanced metering infrastructure (AMI) which allows communications between smart meters deployed at consumers' buildings and an electric utility (EU).

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

This communication is essential for billing, energy, and load management [4]. Contrary to receiving the power consumption readings on a monthly basis in the traditional power grids, smart grids allow transmission of fine-grained readings from smart meters periodically (usually every few minutes) [5], and in this case, it is called periodic-transmission AMI or ''PT AMI''. The EU uses these readings for efficient energy management, bill estimation, and load management.

However, reporting power consumption readings periodically results in enormous data transmission between smart meters and the EU, and because AMI contains millions of smart meters, the problem exacerbates [6]. This limitation results in an ineffective utilization of the available communication bandwidth and because cellular networks are usually used to transfer readings from smart meters, transmitting a huge volume of data becomes expensive [7]. Therefore, a more efficient approach to collect power consumption readings without overbearing the communication network is the change-and-transmit (CAT) approach [8]. Here, smart meters only transmit fine-grained readings once there is enough difference between the current reading and previously reported reading. This approach is called ''CAT AMI'' [9], [10], [11]. Explicitly, readings are sent if the percentage change in readings is above a predefined threshold. In the case where the change is below the threshold, a reading is not sent by the meter and the EU simply uses the last reported reading. The smart grid is susceptible to power theft through cyber-attacks launched by malicious consumers. In these attacks, consumers hack their smart meters to tamper with the power consumption readings in an effort to have a lower electricity bill. These attacks impair the power grid financially. It has been reported that about $6 billion and $17 billion was lost annually in the U.S [12] and India [13] respectively, all due to power theft. Moreover, these false readings might alter the stability of the power grid as they contribute to making bad (or suboptimal) decisions regarding grid management, energy management, and load monitoring [14]. In extreme cases, it might cause blackouts. Using hardware tamper proof modules in the smart meters to prevent these attacks has several limitations. Specifically, these modules are costly and require full trust which cannot be guaranteed. That is why to detect power theft in AMI networks in the literature, various approaches that do not need tamper proof modules have been proposed. While a Kalman filter is used in [15] to detect electricity theft, most of the existing approaches in the literature are machine learning-based [13], [16], [17], [18], [19], [20], [21]. These solutions use either shallow models [13], [17], [18] or deep learning models [16], [19], [20]. Promising results have been found with deep learning-based solutions since they offer high accuracy in detecting power thefts. Furthermore, the power theft detector can be either generic, i.e., it can be utilized for all consumers, or customer-specific, i.e., a tailored detector is trained for each consumer. Therefore, as opposed to general detectors, customer-specific detectors cannot be employed to detect false-reading attacks until enough historical power consumption readings for each consumer are collected which may be a challenge, especially for new consumers. Additionally, customized detectors are susceptible to contamination attacks, in which new consumers initially send false readings, and in this case, the malicious consumers will not be detected if they continue to report false data [22]. However, *the literature has a research gap in detecting power theft in CAT AMI networks while preserving consumers' privacy* as the existing works are focusing on developing power theft detectors for the periodic transmission AMI networks, and none of the existing works has investigated the privacy-preserving detection of power theft in CAT AMI.

Ibrahem et al. [23] proposed a power theft detector for CAT AMI that can detect malicious consumers. Nevertheless, the scheme does not take into consideration preserving the privacy of the consumers as it uses the CAT readings in clear without any protection, which raises a serious privacy issue. This is because sensitive information can be inferred about the consumers' life habits using these readings, e.g., whether the dwellers are around or on vacation [9], [24], sleeping cycles, mealtimes, number of dwellers, etc. [25], [26]. This information can be misused to commit crimes [27]. Also, insurance companies can adapt their plans for their consumers if they can get this kind of information. Hence, to ensure that consumers' privacy is preserved, encryption schemes must be utilized to conceal the consumption readings while allowing the EU only to utilize the encrypted readings without being able to learn the plaintext readings for power theft detection, energy management, load monitoring, and billing [6]. Therefore, *this paper deals with the issue of detecting power theft in CAT AMI while preserving consumers' privacy by encrypting their readings and enabling the EU to do energy management, load monitoring, and billing using encrypted readings*.

A. SIGNIFICANCE OF RESEARCH

To preserve the consumer's privacy, their power consumption readings must be encrypted and used for billing, energy management and detection of electricity theft without decrypting them, which creates the following challenges: (1) the choice of power theft detection model is controlled by a cryptosystem that can be used to perform the model's operations over encrypted data efficiently. This is because the cryptosystem should enable the EU to utilize the previously transmitted-encrypted readings to evaluate the detector in case there is no reading transmissions, (2) since the power consumption readings are encrypted, malicious consumers can launch new and various types of attacks without considering the threshold of the CAT approach because the EU cannot verify whether the readings follow the CAT approach, (3) the proposed power theft detector in [23] considers consumer's transmission patterns besides their CAT readings to improve the accuracy; however, it cannot be considered while encrypting the consumption readings since malicious consumers can launch power theft cyber-attacks without changing the

transmission pattern, which makes our problem more complicated, and (4) unlike the power theft detector in [23] which is attack-specific, i.e., there is one detector customized for each attack, which needs more computations in training and evaluating the models, a generic attack detector that is employable for different types of attacks should be trained.

This paper tackles the limitations of existing methodologies through a privacy-preserving power theft detection scheme. First, this paper develops a hybrid deep learning power theft detection model for CAT readings, consisting of a combination of feed-forward, gated recurrent unit, and convolutional neural networks. The input of the model is the power consumption CAT readings of one day and the output is whether the readings are false or not. Then, this paper develops a homomorphic encryption (HE) [28] cryptosystem to enable the EU to do load monitoring, compute bills, and evaluate the model using encrypted CAT readings to preserves privacy. Specifically, each consumer sends encrypted CAT readings and our scheme uses two mathematical operations that can be done over encrypted data including aggregation and dot product. The encrypted readings of one meter over a billing period can be aggregated and only the aggregated value can be known by the EU for billing without being able to compute the individual reading. Similarity, the encrypted readings of the smart meters of one AMI are aggregated to compute aggregated consumption and use it for load monitoring without being able to compute the individual readings. Finally, by exploiting the dot product over encrypted data, our model can be evaluated through the encrypted CAT readings without exposing these readings to the EU. In order to evaluate the performance of our proposed detector, the paper uses an actual consumption dataset collected by the Smart Project [29], which comprises actual power readings of consumers. Additionally, malicious samples are created by proposing some collection of attacks adapted to CAT AMI, and the proposed detector is general and can be applied to all consumers.

In this paper, the following primary contributions are demonstrated.

- Our research is the first to explore the detection of power theft in AMI networks that utilize the CAT approach while preserving the privacy of consumers. Most of the previous methods of power theft detection have utilized the PT approach, which requires the receipt of all readings to be used for detection and have not taken into account the potential for readings not being received due to the CAT approach. To the best of our knowledge, none of the existing works has investigated the privacy preserving detection of power theft in CAT AMI.
- Since preserving consumers' privacy, in the CAT AMI, is more challenging as clarified earlier, new attacks can be launched since the attackers can deviate from the CAT approach when transmitting the readings and it is not possible for the EU to ascertain whether the readings comply with the CAT approach, as they are encrypted. Consequently, this paper proposes a set of power theft attacks specifically designed for CAT AMI networks to generate malicious samples.
- A dataset for CAT AMI is created and used to train a detector for power theft attacks.
- To evaluate our proposals, extensive experiments and analysis are conducted. The results demonstrate that our proposed power theft detector has the ability to accurately detect malicious consumers with acceptable overhead while preserving the privacy of the consumers.

TABLE 1. Key notations and abbreviations used in the paper.

Notation	Represent for
AMI	Advanced Metering Infrastructure
CAT	Change and Transmit
EU	Electric Utility
HE	Homomorphic Encryption
PT	Periodic Transmission
SM	Smart Meter
KDC	Key Distribution Center
$f_i(\cdot)$	The functions of attack i
Th_{act}	The CAT approach threshold
r_l^i	The previous reported reading of smart meter SM_i
r_c^i	The present true power consumption of SM_i
x_l^i and x_u^i	The upper and lower limits of the CAT approach
Th_u and Th_l	The upper and lower thresholds used in attack #5
$\eta\%$	The reduction factor for Attack #1
β	The reduction factor for Attack #2
$m_i[t]$	Masked power consumption reading of SM_i at time slot t
$C_i[t]$	The homomorphic encryption of $m_i[t]$
$\lvert\mathbb{SM}\rvert$	The total number of smart meters in an AMI
x_{agg}/Y_{agg}	The private/public key pairs of the aggregator
x_i/Y_i	The private/public key pairs of SM_i
$r_i[t]$	A random number selected by SM_i at time t used in the computation of the encryption
$\sigma_i[t]$	The signature of SM_i at time t
$H()$	Hash function where $H:\{0,1\}^* \rightarrow \mathbb{U}$
$S_i[t]$	The sequence number of SM_i at time t
$C_{agg}[t]$	The encrypted aggregated reading of an AMT at time t
$\hat{e}(\cdot,\cdot)$	Bilinear Pairing
$\mathbf{c}_i^B$	A vector for the encrypted readings of SM_i for the billing period T_B
$\mathbf{c}_i^D$	A vector for the encrypted readings of SM_i for the model evaluation period T_D
$C_{agg}^b[i]$	The encrypted aggregated readings of SM_i over the billing period T_B

The following is the paper's organization; section II elucidates the related works while section III explains the design objectives and system model. Section V discusses preliminaries utilized in our research. In Section IV, the dataset used to train and evaluate our detectors is presented. Section VI outlines our envisioned scheme, and Section VII discusses its performance evaluation. Finally, Section VIII concludes the paper. The main notations and abbreviations used in this paper are given in Table 1.

II. RELATED WORKS

Privacy concerns have arisen due to the ability to extract personal data from fine-grained power consumption readings provided by smart meters, using nonintrusive techniques for appliance load monitoring. Increasing the time intervals between consumption measurements is expected to enhance privacy. In [30], the research investigates how the granularity

of consumption data impacts edge detection methods, which are commonly employed in nonintrusive load monitoring algorithms. The study reveals that the detection rate for appliance usage decreases when the time interval exceeds half the duration an appliance remains active.

Smart grids have emerged as a crucial solution for electricity infrastructure, primarily due to the significant rise in electricity prosumers-consumers who also produce energy. In the context of a competitive energy trading market within a Neighborhood Area Network (NAN), the research discussed in [31] presents a framework that safeguards the confidentiality of prosumers' identities and offers protection against traffic analysis attacks. Furthermore, the proposed framework conceals both the number of bidders and the number of successful bids from malicious attackers.

Different works have been proposed in machine learning-based power theft detection [13]- [24] using periodic transmission of readings in AMI network. However, these works do not consider preserving the consumers' privacy in their various networks. Jokar et al. [13] employed the Irish dataset [32] for training user-specific power theft detectors. The detector was trained for individual consumer using his power consumption readings. Jokar et al. used two experiments in training the detector. In the first experiment, benign samples of each consumer were utilized to train an SVM-based detector. Both benign and malicious samples were used in the second experiment. Since Irish dataset does not comprise of malicious data, some attacks were developed to generate synthetic malicious data. Results showed that the detector trained in the second experiment outperformed greatly the detector trained in the first experiment.

Deep learning approaches were used by Buzau et al. [20] and Zheng et al. [16] where a generic power theft detector was developed by the use of datasets in Endesa [20] and the State Grid Corporation of China (SGCC) [33]. The SGCC dataset comprises of benign and malicious data. The model in [16] uses deep learning model which consists of convolutional neural network (CNN) and multilayer perceptron (MLP) components so that the electric consumption periodicity is captured. It was observed from the statistical analysis done on the SGCC dataset that the malicious consumers' consumption readings tend to be less consistent/periodic when compared to those of benign consumers. So, the temporal relationship of the power readings is learned by the detector to help with identifying false readings. Furthermore, a deep learning model which composes of MLP and long short-term memory (LSTM) modules was also used in [20]. The results in the two works show that the detection accuracy of [20] was better than [16].

In [34], a privacy-preserving approach to the detection of manipulated Distributed Energy Resources (DER) power generation readings is proposed. The proposed approach aims to detect malicious actors that report false power generation readings for financial gain. The proposed method uses the fact that the (normalised) power output from photovoltaic (PV) installed in a geographical area should be similar, and thus deviations from the norm demonstrates malicious activities. Specifically, the approach calculates the Euclidean distance between all pairs of normalised power generation readings. The paper uses a clustering technique to find the outlying distances that indicate malicious activities. Homomorphic encryption is used to compute the Euclidean distances over encrypted data and share the encrypted result with a third party to detect electricity theft with privacy preservation.

In [35], a privacy-preserving federated learning approach for energy theft detection in smart grid is proposed. Federated learning is used to enable different owners of datasets to train a global model trained on their data without revealing the dataset to preserve privacy. Unlike this paper that aims at preserving privacy during the training stage of the electricity theft detector, our paper aims at preserving privacy during the evaluation stage of the detector, and therefore, the approach proposed in [35] complements our proposed scheme.

Smart micro-grid (SMG) networks are small scale distributed electricity provision networks that are based on a distributed renewable power generation and a low-cost communication infrastructure. SMGs are used to enhance the reliability of the smart grid. Because of the low-cost devices used in SMG, they do not have enough computation resources to use cryptography to protect the confidentially of the data exchanged. Therefore, in [36], a differential privacy (DP) based technique is proposed to protect privacy. However, DP-based technique adds noise to the data to preserve privacy and there is a trade-off between the level of privacy preservation and the utility of the data, i.e., adding more noise enhances the privacy preservation level but with less utility of the data. Instead, in this paper, a different approach is used in which the exact data are used but in ciphertext domain to preserve privacy, i.e., the encrypted readings can be used to do load monitoring, billing, and evaluating the electricity theft detectors using encrypted reading and no one is able to obtain the plaintext readings.

Some works has investigated the use of CAT approach in smart grid [37], [38], [39], [40], [41]. Samarakoon et al. [37] studied demand/response using the CAT approach, [39]-[41] investigated finding the right value for the threshold. Nonetheless, their models were not concerned with consumers' privacy thereby making the models prone to attacks. Moreover a CAT approach is used in [42] to reduce the overhead in federated learning by not sending gradients that do not change enough.

Ibrahem et al. [23] proposed a generic theft detection of CAT AMI using Irish dataset. The model uses a hybrid deep learning scheme that comprises of CNN, fully connected FFN and a GRU. The dataset was modified so as to follow the CAT architecture by clipping the consumption readings against a predefined threshold. The CNN and GRU were employed in extracting crucial features from the inputted CAT power consumption readings. The FFN was used for the model classification. Since the consumption of the consumers

has an impact on the transmission patterns, the detector was improved by applying the transmission pattern along with the CAT power readings to provide an accurate classification of consumers. Furthermore, attacks used in the scheme were also modeled to follow the CAT architecture. The results showed that the detector can identify power theft with high performance and accuracy. However, the scheme does not consider preserving the privacy of the consumers.

Existing power theft detection schemes in the privacy preservation domain assumed that power readings are reported periodically by the smart meters even when there is no significant difference in the readings. Privacy-preserving data aggregation techniques are used in these schemes to allow the smart meters to send fine-grained encrypted readings and the EU to acquire the accumulated readings for billing, energy and load management without allowing the EU to access each consumer's readings to ensure privacy preservation.

Machine learning models were developed in [43] and [44] to detect power thefts while preserving privacy. A CNN model was proposed in [43] in which smart meters transmit their encrypted readings to a fully trusted system and distrusted system. The trusted system evaluates a CNN model on the decrypted power readings in order to detect power thefts. The output of the model is then reported to the EU for necessary action. The distrusted system collects the aggregated encrypted readings in the network without learning the consumers' readings so as to preserve privacy. These aggregated readings are used for load monitoring. Practically, it cannot be guaranteed that a system can be fully trusted and it cannot compromise consumers' information.

Nabil et al. [44] developed a privacy preserving deep learning power theft detection scheme. The smart meters mask their power consumption readings using secret sharing technique and the EU uses the aggregated masked readings to compute the aggregated readings for billing and energy management without learning the individual readings. A multi-party computation protocols that are evaluated with the use of arithmetic and binary circuits were employed on a convolution neural network model. The CNN model's evaluation can only be done through an interactive/online session between individual smart meter and the EU. Furthermore, the scheme's model classification is both known to the EU and smart meters. However, this scheme suffers from high computation and communication overheads. Most of the overheads are incurred through the continuous linear approximation of the nonlinear (sigmoid) function used in the scheme, and because the model is evaluated on each smart meter, high computation overhead arises. Furthermore, high overhead is also accrued using the secret sharing technique i.e., the cost of masking the consumption readings of consumers.

Ibrahem et al. [7] addressed these limitations in [44] by offering a privacy preserving power theft detection that uses a functional encryption (FE) to mask the fine-grained consumption readings. The EU utilized the aggregated encrypted readings for load management, and to compute the electricity bills without learning the consumers' readings. The EU utilizes a functional decryption key and feedforward neural networks (FFN) to detect power theft. Smart meters encrypt their consumption readings and send the ciphertexts to the EU. The smart meters do not require an interactive session in order to evaluate the power theft detector. To ensure privacy is being preserved, no entity within the AMI network is allowed to learn the readings of consumers. The results gotten indicated that the scheme can accurately detect power theft while preserving consumers' privacy with satisfactory communication and computation overheads. The scheme reduced the computation overhead by 97.4 percent better than [44] with low communication overhead.

III. SYSTEM MODELS AND DESIGN GOALS

The proposed network model, threat model and design objectives are discussed in this section.

A. NETWORK MODEL

The AMI network consists of smart meters, Electricity Utility (EU) and a key distribution center (KDC) as shown in the Fig 1. The purposes of each entity are as follows.

- Smart Meters: They are installed at consumers' premises to record and transmit consumers' consumption readings to the EU according to the CAT approach. Only when the current reading exceeds or falls short of the last reported measurement by a set threshold do smart meters communicate readings. In periods where no enough change is recorded, the last reported reading will be used by the EU. Smart meters can either communicate with the EU directly or through a gateway (aggregator).
- Key Distribution Center (KDC): Encryption and decryption keys are generated by KDC which are used by the smart meters and the EU. The KDC is usually managed by a trusted authority like the Department of Energy.
- EU: It receives fine-grained readings from the smart meters, and uses them to compute bills, manage energy, and monitor loads. In addition, it utilizes these readings to evaluate a deep learning model to identify malicious consumers who steal power.

Moreover, Fig. 2 shows the step-by-step process of CAT AMI. Each smart meter first measures the power consumption and then computes the absolute change in the consumption comparing to the last reading reported to the EU. If the absolute change does not exceed the threshold of the CAT approach, the meter does not transmit a reading and the EU uses the last reported reading in the load management, billing, and theft detection. On the other hand, if the absolute change exceeds the threshold of the CAT approach, the smart meter encrypts the reading using homomorphic encryption and transmits the encrypted reading to the EU. For instance, if the last reported readings is $10KWh$ and the threshold is 10%, the meter does not send a reading when the consumption is between $10KWh \pm 1KWh$, and in this case, the EU uses $10KWh$ in the computation, and thus, the maximum error

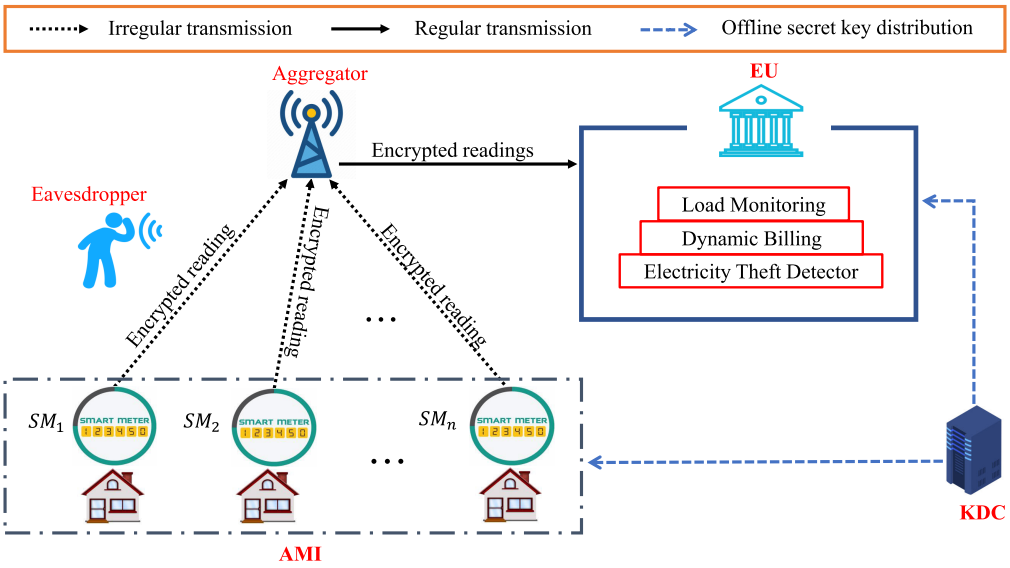

FIGURE 1. Network model of CAT AMI.

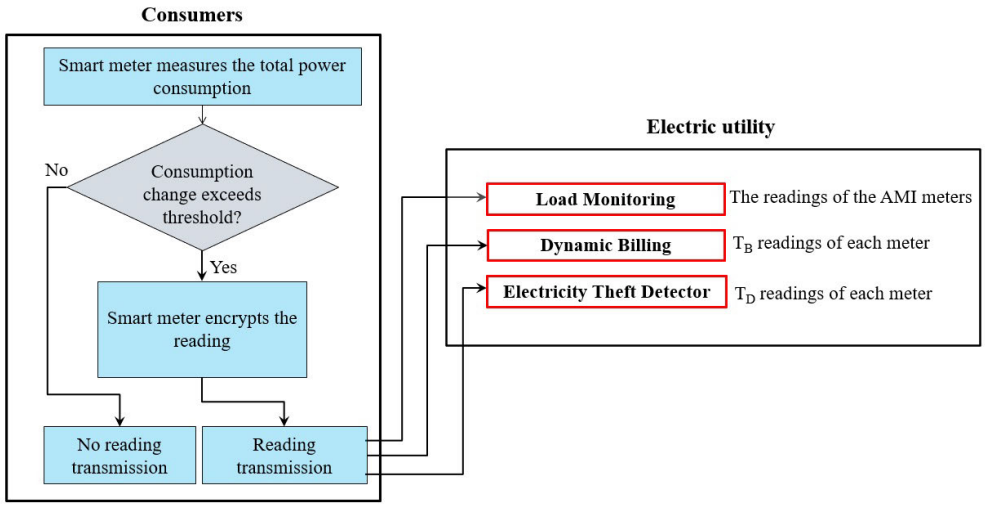

FIGURE 2. Step-by-step process of CAT AMI.

in the readings is $\pm 1KWh$. On the other hand, the meter transmits the readings when the consumption is greater than $11KWh$ or below $9KWh$. At the EU side, it computes the bills using the aggregated T_B readings of each meter, aggregates all the readings of the AMI meters for load monitoring, and uses the ciphertexts of T_D readings of each meter to evaluate the electricity theft detector.

B. THREAT MODEL

In this paper, two types of threats are considered. In the first type, malicious consumers manage to hack their smart meters and change its firmware to unlawfully reduce their bills by reporting false readings to the EU, which may not only cause economic loss to the power grid, but it could lead to wrong decision-making in the energy management of the grid. There are several limitations to using hardware tamper-proof modules in smart meters as a means to prevent these attacks. Specifically, these modules are costly and require full trust which cannot be guaranteed. In the second type of threat, attackers may attempt to acquire the consumption readings of fellow consumers in order to deduce sensitive information about them. The EU may attempt to infer sensitive information about the activities of the consumers from the fine-grained readings received from the smart meters. Furthermore, the malicious consumers could either collude with the EU to deduce the readings of fellow consumers or collude with other consumers in the network to deduce sensitive information of fellow consumers in the network.

C. DESIGN OBJECTIVES

This paper aims to accomplish these security and functionality requirements.

1) Functionality requirements
   - F1: Our solution shall permit the EU to calculate the overall consumers' power consumption in the CAT AMI network at every reporting period for both grid and load management.
   - F2: Our solution shall enable the EU to calculate the electricity bills of each consumer in the network by computing the aggregated consumption of the consumers using their fine-grained readings.
   - F3: Our solution shall enable the EU to detect honest and fraudulent consumers by running the power theft detector on individual consumers utilizing their reported fine-grained consumption readings.
2) Privacy and Security Requirements.
   - *Detection of power theft*: Our detector shall accurately detect any attacks from malicious consumers who intend to steal electricity without being detected.
   - *Consumers' bills and total power consumption confidentiality*: Only EU will be allowed to learn the overall consumption of consumers for load management and also the individual bills of the consumers.
   - *Consumers' privacy preservation*: No entity within the network, including the EU, will be allowed access the plaintext consumers' consumption readings.

IV. DATASET PREPARATION

This section explains the dataset used in training and evaluating the performance of our theft detectors. A benign CAT AMI dataset is created by utilizing various thresholds on benign consumption readings of a publicly available dataset [45]. A collection of power theft cyber-attacks are proposed to create malicious data samples. Lastly, this section explains how the benign and malicious datasets are used in training the proposed detectors.

A. BENIGN DATASET

The CAT dataset are prepared from Smart Project dataset [45] which contains PT transmissions. It is an open-access smart meter dataset containing benign power consumption readings of 114 apartments. These readings are reported to the EU per minute. Two new datasets Y_5 and Y_{10} from this dataset are created by applying different transmission rates of $1/5min$ and $1/10min$ thereby producing 288 readings per day and 144 readings per day respectively. In total, 39,786 benign samples were produced with each sample containing the consumer's readings per day.

Furthermore, other datasets are created for our CAT approach using the earlier created two dataset Y_5 and Y_{10}, by varying the threshold at 5% and 10%. This means that when using the 5% threshold or the 10% threshold, a smart meter only sends a power consumption reading when the absolute change in the consumption comparing to the last reading meets those thresholds. The following formula was used to compare the CAT technique to sending data periodically at various transmission speeds and thresholds in order to assess the percentage of unreported readings and determine the savings gained of the CAT approach.

$$S = \frac{(P - C)}{P} \times 100 \tag{1}$$

where S is the savings gained, P is the number of reported readings when using PT approach, C is the number of reported readings when using the CAT approach. Table 2 shows the bandwidth savings gained by utilizing the CAT technique at various transmission rates and thresholds. It is worth noting that when the threshold rises, the possibility of the consumption change exceeding the CAT approach's threshold lowers, resulting in fewer transmissions. However, the savings reduce as the interval of transmission increases due to the increased possibility of the change in consumption exceeding the threshold thereby causing more transmissions to occur.

TABLE 2. Savings gained using the CAT approach at different transmission rates and thresholds.

Transmission Rates	Threshold (%)	
	5	10
5 min	36.48	39.75
10 min	19.95	25.87

The CAT approach necessitates that the EU accepts clipped readings from smart meters in the network. This leads to a reading error because the readings received by the EU could be less or more than the real readings recorded by the smart meters owing to the usage of thresholds. Our network comprises of 114 smart meters, and the aggregated readings for the individual consumers which is then used to compute their bills are computed. Furthermore, the EU is allowed to compute the aggregated readings of the whole collections of smart meters which is used for load monitoring and energy management. Then, the error due to using aggregated readings is also determined. Consequently, the error due to using aggregated readings for load management is shown figure 3 for various thresholds and transmission rates by the cumulative frequency function (CDF). Figure 4 shows the aggregated readings' error incurred in billing for two consumers selected at random. From the two figures, the error from the aggregated readings is substantially lower than the error from the highest individual reading since some errors are negative and others are positive thereby reducing the overall reading error. As a result, even when the readings received by the EU are clipped due to using the CAT approach, the EU can still utilize these readings for accurate load monitoring and billing.

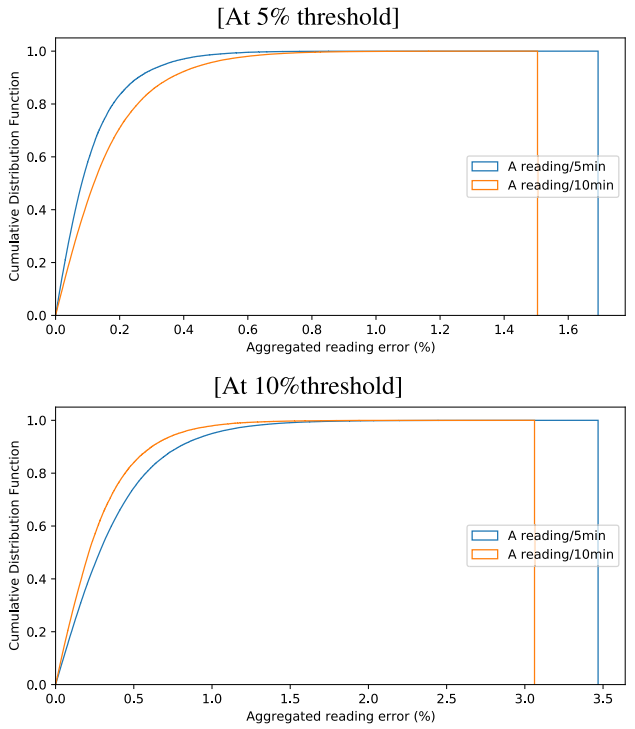

FIGURE 3. CDF of error for aggregated reading for load monitoring of different transmission rates and thresholds.

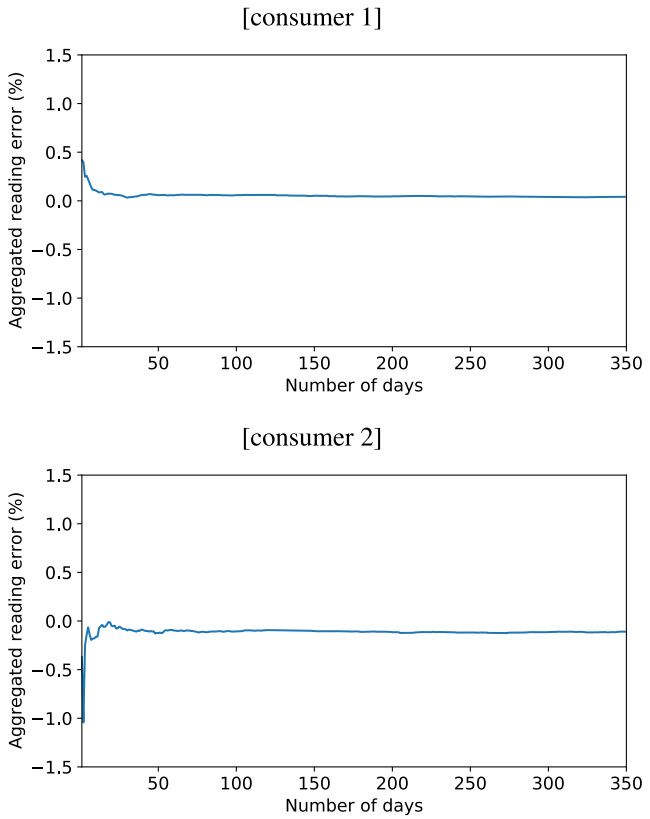

FIGURE 4. Aggregated readings error for two consumers randomly chosen.

B. MALICIOUS DATASET

In this study, our proposed model is trained on both malicious and benign data samples. The malicious data samples are developped by implementing a collection of attacks that may be carried out by malicious consumers in the CAT AMI networks because there were no real malicious data samples available. In order to lower the electricity bills through a cyberattack, malicious consumers reduce the values of their reported readings. Five attacks are developed for our malicious samples and applied them on the benign dataset. Table 3 shows a summary of the attacks in which all attack functions $f(\cdot)$ aim at reducing electricity bills. Denote Th_{act}, r_l^i, and r_c^i as the CAT approach threshold, the previous reported reading of SM_i and the present true power consumption, respectively. So, the following condition should meet to send a reading $(x_l^i > r_c^i > x_u^i)$, where $x_l^i = r_l^i - (r_l^i * Th_{act})$ and $x_u^i = r_l^i + (r_l^i * Th_{act})$ are corresponding to the upper and lower limits, respectively.

Attack 1, as seen in Table 3, lowers the readings by $\eta\%$ when there is a transmission and the current reading r_c^i is greater than x_u^i, otherwise, the true power reading is reported. Therefore, rather than taking the real consumption r_c^i into account, which is greater than the reported reading, this attack makes the EU use a reduced reading $\eta \times r_c^i$ when $r_c^i > x_u^i$. Additionally, since certain readings are correct (when $r_c^i < x_l^i$), this attack seeks to trick the power theft detection while lowering the bill. Attack 2 compares the previous reported reading r_l^i with the current reading r_c^i, and reduces the lowest reading by β. Similar to Attack 2, Attack 3 also compares the previous reported reading r_l^i with the current value r_c^i but the attacker sends the lowest reading only. In this attack, rather than considering the correct present consumption r_c^i, when $r_c^i > x_u^i$, the EU utilizes the most recently reported reading r_l^i that is less than r_c^i. Also, Attack 3 is intended to create confusion in the power theft detector while simultaneously causing decrease in billing since certain readings are genuine (in the case that $r_c^i < x_l^i$).

TABLE 3. Function for the proposed cyberattack for power theft in the CAT AMI.

Attacks	Attack function
Attack 1	$f_1(r_c^i) = \begin{cases} \eta \times r_c^i & r_c^i > x_u^i \\ r_c^i & otherwise \end{cases}$
Attack 2	$f_2(r_c^i) = \begin{cases} \beta \times r_c^i & r_c^i < x_l^i \\ \beta \times r_l^i & otherwise \end{cases}$
Attack 3	$f_3(r_c^i) = \begin{cases} r_c^i & r_c^i < x_l^i \\ r_l^i & otherwise \end{cases}$
Attack 4	$f_4(r_c^i) = \begin{cases} 0 & \forall t \in [t_s, t_f] \\ r_c^i & \forall t \notin [t_s, t_f] \end{cases}$
Attack 5	Choose asymmetric thresholds Th_l and Th_u, where $Th_l = Th_{act} \times \alpha_l$ and $Th_u = +h_{act} + \alpha_u \times Th_{act}$ $f_5(r_c^i) =$ $\begin{cases} \text{Transmit } r_c^i & otherwise \\ \text{Do not transmit} & r_l^i - r_l^i * Th_l < r_c^i < r_l^i + r_l^i * Th_u \end{cases}$

Attack 4 is a By-pass attack, whereby a malicious consumer transmits readings of zero over a predetermined time period (i.e., $[t_s, t_f]$), and in the other time periods, it sends the correct consumption reading r_c^i following CAT approach, where t_f is the start of the power theft interval and t_s is the end of the power theft interval.

Alternatively, rather than adhering to the actual symmetrical threshold Th_{act} determined for the CAT approach, i.e., $\pm 5\%$, Attack 5 attempts to establish and adhere to asymmetric threshold boundaries, denoted Th_u and Th_l. For example, Th_l is equal to 5% while Th_u is equal to 10%, with Th_l and Th_u representing the threshold's lower and upper boundaries that are set by the attacker, respectively. The values of Th_l and Th_u are chosen by the attacker while making sure that $|Th_u| > |Th_l|$ to guarantee a decreased bill. In this attack, a reading is reported when $r_c^i < r_l^i - r_l^i * Th_l$ or $r_l^i + r_l^i * Th_u < r_c^i$. As the Th_u increases, it is less likely that the current consumption will exceed Th_u, leading the EU to consider the lower last reported consumption r_l^i for a longer period, in order to reduce the bill. This means that r_c^i is higher than r_l^i, and hence, r_c^i will only be sent if there is a considerable change between the most recent reading and the previous one, thus guaranteeing a reduced bill.

C. DATA PRE-PROCESSING

To generate malicious data samples, the parameters for the attacks discussed above are set in a random manner based on uniform distribution as follows. η and β, in functions $f_1(\cdot)$ and $f_2(\cdot)$, are randomly chosen over the interval [0.3, 0.8], where as η decreases, profits that the attacker can achieve increases. In $f_4(\cdot)$, t_s is a random variable in [0, 80] while the attack's period, i.e., $t_f - t_s$ is chosen in [40, 80]. For function $f_5(\cdot)$, α_l and α_u are randomly chosen over the interval [0.05, 0.2] and [3, 8], respectively. As α_u increases (i.e., Th_u increases), more bill reduction is accomplished due to the fact that as the Th_u is bigger, it becomes less likely that r_c^i exceeds Th_u, leading the EU to consider r_l^i for a longer period, in order to reduce the bill.

Given that our dataset contains benign CAT readings of one hundred and fourteen consumers over 349 days, the total number of benign samples is 39,786 (114*349). For a 1/10min transmission rate, there are 144 CAT readings in each sample that is either labeled one if it is malicious or zero if benign. The five attacks are then employed to generate five malicious samples per benign sample, yielding 349 honest records as opposed to 1, 745 malicious records (i.e., 5 *attacks*$\times$349) for each SM. The result is an imbalanced dataset because there are more malicious samples than honest samples. The problem of data imbalance is addressed by balancing the size of the benign and malicious samples using an adaptive synthetic sampling approach (ADASYN) [46]. As a result, there are 3, 490 malicious and honest records in each SM, with 144 CAT readings in each record. Hence, our dataset contains approximately 500, 000 records for 144 SMs. The dataset is then further split into two portions, with 20% of the samples being used for evaluating our detector and 80% of the samples being utilized for detector training.

V. PRELIMINARIES

This section briefly discusses the cryptosystems, deep learning systems and the activation functions used in this paper.

A. BILINEAR PAIRING

A pairing is admissible if the mapping is non-degenerate and computable. Bilinear pairing will be used to verify the smart meter's signatures efficiently. Given that U and U_T are cyclic groups of the large prime order y, and Q, V are generators of U. A pairing is a mapping of $\hat{e} : U \times U \rightarrow U_T$ satisfying the property of bilinearity. This means

$$\hat{e}(V, V) \neq 1_{U_T}$$
$$\hat{e}(cV_1, dQ_1) = \hat{e}(V_1, Q_1)^{cd} \in U_T,$$

for all $c, d \in Z_q^*$ and any $V_1, Q_1 \in U$

B. HOMOMORPHIC ENCRYPTION

Paillier cryptosystem is a homomorphic encryption scheme that permits arithmetic operations to be performed on aggregated encrypted data without decrypting these data. This cryptosystem consists of three processes

- Encryption: given that $r \in Z_n^*$, $E(\cdot)$, and $m \in Z_n$ are a randomly generated number, encryption function, and the plaintext or message respectively. The encrypted message can be computed as:

$$f = E(m) = g^m r^n \mod n^2 \tag{2}$$

- Decryption: let the encrypted message $f \in Z_{n^2}^*$, the message is

$$D(f) = m = L(f^\lambda \mod n^2) \cdot \mu \mod n \tag{3}$$

- Key generation: The public key is generated by choosing prime numbers q_1 and p_1, where $|q_1| = |p_1|$, followed by computing λ and n through $\lambda = lcm(p_1 - 1, q_1 - 1)$ and $n = q_1 p_1$.
  Furthermore,

$$\mu = \frac{modn}{L(g^\lambda \mod n^2)} \tag{4}$$

  where, a generator $g \in Z_{n^2}^*$ and $L(u) = ((u-1)^{-1} \times n)$. Hence, the private key is $sk = (\mu, \lambda)$ and its corresponding public key is $pk = (g, n)$.
  Homomorphic encryption is used to preserve the consumers' privacy by evaluating our detector using enecrypyted data while enabling the EU to aggregate the consumers' readings in the CAT AMI network.

C. DEEP LEARNING

A deep learning network comprises of input layer, hidden intermediate layer, and output layer. Supervised learning is a kind of deep learning which involves the use of labelled dataset to train a model. Typical ways by which supervised

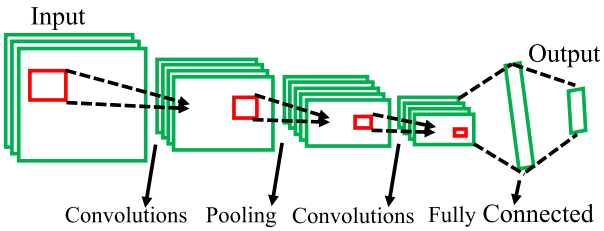

FIGURE 5. Architecture of a convolutional neural network.

learning are implemented are through MLP, CNN and recurrent neural network (RNN). Deep neural networks are usually trained by learning weights and bias parameters. Features extracted from input data are mapped into higher abstraction in the intermediate layers through feed forward and back-propagation. During back propagation, the learning is done by calculating the cost function and choosing an optimiser and the output layer utilizes these mapped abstractions for classification. Using the cost functions' gradients, the bias and weights of parameters in the intermediate layers are updated at every iteration. The output values are then equated to the correct values to optimize the cost function, and the difference in value is then sent via the hidden layers' neurons to alter the weights associated with each connection, resulting in a cost function that is eventually minimized. *Categorical cross-entropy C(z,ẑ)* is the cost function used in the classification tasks and it is a measure of the loss as a result of the change in the learned distribution $\hat{z}$ and true distribution z for P classes.

$$C(z, \hat{z}) = \min_{\theta}(-\sum_{c=1}^{P} z(c) \cdot \log \hat{z}(c)) \tag{5}$$

The labeled data and cost function are then optimized using an optimization method. Furthermore, using the k-fold cross validation method, hyperopt, etc., the model may be tweaked for improved performance by changing hyper-parameters like optimizer's type, the number of layers, and each layer's neurons number.

D. CONVOLUTIONAL NEURAL NETWORK (CNN)

Since its advent, CNN has been employed in varieties of applications ranging from speech processing, autonomous driving applications, image processing etc. This is owing to its capability to extract complex patterns or features from input data. Fig. 5 shows the architecture of a typical CNN. The convolutional layer of CNN is made up of filters, which slide across the input data so as to extract distinctive features. In order to conduct complex decisions and accomplish complicated tasks, these features are made to pass via a Rectified Linear Unit (ReLU), Sigmoid function or Tanh depending on the nonlinear function used. Furthermore, by subsampling the feature map, pooling layers help to compress the convolution layer's output. This subsampling ensures that important information are retained [47], [48]. Fully connected layers process these extracted features from the pooling layers for decision making purposes.

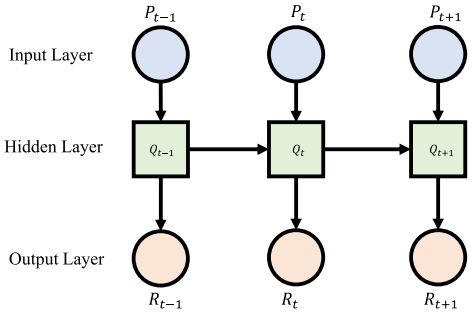

FIGURE 6. Architecture of a GRU neural network.

E. GATED RECURRENT UNIT (GRU)

It is a type of RNN capable of memorizing long sequence of input patterns. The memorization of information is achieved by employing hidden states and forming a directed graph of the relations between internal units. The transition function utilizes the present information P_t and the previous state Q_{t-1} at each time step t as shown in Fig. 6. It computes the present hidden state as

$$Q_t = F(P_t, Q_{t-1}), \tag{6}$$

where F is a nonlinear transformation such as Sigmoid and Tanh functions. Q_{t-1} is referred to as the memory of previous state. Due to the recurrent structure, GRU is said to recall previous inputs of the network. The reset and update gates are used by GRU to control the flow of information and to determine the data to be saved and the date to be deleted. Therefore, GRU can capture the correlation between the inputs making it very useful in our application to capture the correlation in the power consumption readings. Moreover, GRU is employed in speech synthesis, text generation, and speech recognition.

F. ACTIVATION FUNCTIONS

Activation functions are utilized to convert a neuron's aggregated weighted input into the neuron's activation. They contribute immensely to the convergence speed and model accuracy. Here are the commonly used activation functions.

- SoftMax: It is usually utilized in multi-class classification of data. It calculates a probability vector for any input vector $x = [x[1], x[2], x[3] \ldots x[N]] \in R^N$ of length of N number of classes.

$$softmax(x[k]) = \frac{e^{x[k]}}{\sum_{j=1}^{N} e^{x[j]}} \tag{7}$$

  for $k = \{1, 2, 3, \ldots N\}$
- Rectified linear unit (ReLU):): If given a positive input, ReLU yields the same output; otherwise, it yields zero. This is because it only performs max function on the input. This activation function is highly efficient.

$$ReLU(x) = \max(0, x) \tag{8}$$

VI. METHODS

This section first provides an overview for our scheme and then explain the different phases iincluding initialization,

reporting of smart meters' consumption readings, aggregating the readings using their ciphertexts, and decrypting the aggregated readings by the EU to perform load monitoring. The section, then, discuss the process of training a deep learning model for detecting power theft, as well as the way the EU utilizes the encrypted readings to evaluate our detector without compromising the privacy of consumers.

A. OVERVIEW

Here are the main stages of our proposed scheme.

1) At the time slot t, each $SM_i \in \mathbb{SM}$ encrypts its masked power consumption reading $m_i[t]$ by using homomorphic-based Paillier cryptosystem if there is enough change in the consumption. Then, it transmits its encrypted reading $C_i[t]$ to the aggregator.
2) Then, the aggregator collects and aggregates these encrypted readings $C_i[t]$, for $\{1 \leq i \leq |\mathbb{SM}|\}$, from all smart meters, i.e., $\sum_{i=1}^{|\mathbb{SM}|} \boldsymbol{m}_i[t]$, where $\boldsymbol{m}_i[t]$ is the reading from smart meter, SM_i at time slot T_t in an CAT AMI network for load monitoring and energy management.
3) Regarding billing, the aggregator computes the encrypted aggregated reading for each consumer i $\sum_{t=1}^{b} \boldsymbol{m}_i[t]$ at the end of every billing period T_B.
4) At the end of every power theft detection period T_D, the aggregator computes the encrypted dot product of the encrypted CAT readings for this period and the power theft detection model's weights. Then, it sends these results to the EU.
5) All the encrypted results from stages 2, 3, and 4 are sent by the aggregator to the EU for load monitoring, billing computation, and evaluating a theft detection model to identify malicious consumers respectively, without compromising the privacy of consumers, i.e., without learning the consumers' plaintext readings.

B. INITIALIZATION

Our scheme is bootstrapped by an offline KDC as follows. The creation of the Paillier cryptosystem's public key (g, n = pq) and private keys (λ, μ) begins with selecting two large prime numbers, q and p, where they have the same magnitude [28], [49]. This is followed by computing the parameters for bilinear pairing $(\mathbb{U}_T, \mathbb{U}, q_1, \hat{e}, V)$. A protected hash function, $H : \{0, 1\}^* \rightarrow \mathbb{U}$, is selected and the public parameters are published as $pubs = \{q_1, \mathbb{U}, n, V, \hat{e}, g, \mathbb{U}_T, H\}$. Each smart meter SM_i derives a corresponding public key $Y_i = x_i V$ from a private key $x_i \in \mathbb{Z}_q^*$, and the aggregator obtains the private/public key pairs x_{agg}/Y_{agg}.

C. REPORTING OF THE CONSUMPTION READINGS

Once there is an enough change in SM_i's reading, it encrypts this reading $m_i[t]$ and transmits its corresponding ciphertext $C_i[t]$ to the aggregator in a time slot T_t by carrying out the steps outlined below.

- S1: SM_i selects a number randomly $r_i[t] \in \mathbb{Z}_n^*$ and uses the Paillier cryptosystem to encrypt $m_i[t]$ as follows.

$$C_i[t] = g^{m_i[t]} \cdot (r_i[t])^n \mod n^2 \tag{9}$$

- S2: SM_i computes a signature σ_i for $C_i[t]$ and a sequence number $(S_i[t])$ using its secret key x_i as

$$\sigma_i[t] = x_i H\left(C_i[t] \| S_i[t]\right), \tag{10}$$

  where the sequence number is used to secure against replay attacks and also enable the aggregator to identify dropped messages and in this case it can ask for retransmission.
- S3: the aggregator receives this tuple from SM_i.

$$C_i[t] \, \| S_i[t] \| \, \sigma_i[t] \tag{11}$$

D. AGGREGATION OF ENCRYPTED READINGS

In order to validate the smart meters' readings and compute the ciphertexts of the aggregated readings of the smart meters, an aggregator must save the most recent encrypted reading transmitted by each SM so that it can be used if the smart meter does not transmit an encrypted reading in next time slot when the consumption does not change enough. The aggregator should then carry out the following procedures.

1) Verification of the received messages: The aggregator should first verify the freshness of the received message timestamps, and then perform batch verification of the received signatures using the following equation:

$$\hat{e}\left(\sum_{i=1}^{k} \sigma_i[t], V\right) \stackrel{?}{=} \prod_{i=1}^{k} \hat{e}\left(H\left(C_i[t] \| S_i[t]\right), Y_i\right) \tag{12}$$

where the number of messages is $k \leq |\mathbb{SM}|$.

1) PROOF OF SIGNATURE VERIFICATION

$$\begin{aligned}
\hat{e}\left(\sum_{i=1}^{k} \sigma_i[t], V\right) &= \prod_{i=1}^{k} \hat{e}\left(\sigma_i[t], V\right) \\
&= \prod_{i=1}^{k} \hat{e}\left(x_i H\left(C_i[t] \| S_i[t]\right), V\right) \\
&= \prod_{i=1}^{k} \hat{e}\left(H\left(C_i[t] \| S_i[t]\right), x_i V\right) \\
&= \prod_{i=1}^{k} \hat{e}\left(H\left(C_i[t] \| S_i[t]\right), Y_i\right).
\end{aligned}$$

2) The aggregator calculates the encrypted aggregated reading $C_{agg}[t]$ using the ciphertexts of the encrypted readings sent by the smart meters using the following equation.

$$C_{agg}[t] = \prod_{i=1}^{|\mathbb{SM}|} C_i[t] \mod n^2 \tag{13}$$

3) The aggregator utilizes its private key x_{agg} to calculate the signature in the following way.

$$\sigma_{agg}[t] = x_{agg} H\left(C_{agg}[t] \| S_q[t]\right) \tag{14}$$

4) The EU receives the message containing an encrypted aggregated reading, a sequence number, and a signature from the aggregator in a tuple form:

$$C_{agg}[t] \| S_q[t] \| \sigma_{agg}[t] \tag{15}$$

E. RECOVERY OF AN AGGREGATED READING

The EU checks whether the sequence number is fresh or not and also validates the signature upon receiving the message from the aggregator through

$$\hat{e}\left(\sigma_{agg}[t], V\right) \stackrel{?}{=} \hat{e}\left(H\left(C_{agg}[t] \| S_q[t]\right), Y_{agg}\right) \tag{16}$$

1) PROOF OF SIGNATURE VERIFICATION

$$\begin{aligned}\hat{e}(\sigma_{agg}[t], V) &= \hat{e}(x_{agg} H(C_{agg}[t] \| S_q[t]), V) \\ &= \hat{e}(H(C_{agg}[t] \| S_q[t]), x_{agg} V) \\ &= \hat{e}\left(H\left(C_{agg}[t] \| S_q[t]\right), Y_{agg}\right).\end{aligned}$$

The EU then utilizes the private key (μ, λ) to decrypt $C_{agg}[t]$, thus allowing for the retrieval of the total consumption reading of the smart meters, which is done through the following operations.

$$D\left(C_{agg}[t]\right) = L\left(C_{agg}[t]^{\lambda} \bmod n^2\right) \cdot \mu \bmod n = \sum_{i=1}^{|\mathbb{SM}|} m_i[t] \tag{17}$$

By carrying out the aforementioned computations, $(\sum_{i=1}^{|\mathbb{SM}|} m_i[t])$ which is the aggregate of the consumption readings of all smart meters for time interval T_t can be obtained. Hence, our scheme fulfills functional requirement (F1) by allowing the EU to compute the aggregate of the power readings for load monitoring while protecting consumers' privacy by not having access to the individual plaintext readings

In addition to the steps explained above, the ciphertexts of each SM_i should be stored by the aggregator in a vector $\mathbf{c}_i^B$ so that bills can be calculated over every billing interval T_B as will be discussed in section VI-F, where $\mathbf{c}_i^B$ is:

$$\mathbf{c}_i^B = [C_i[1], \ldots, C_i[b]]^{\top} \tag{18}$$

As will be discussed in section VI-G2, the ciphertexts of each SM_i, over power theft detection interval T_D, should also be stored by the aggregator in vector $\mathbf{c}_i^D$ so that the EU can use them as an input to the detector at the end of each T_D, where $\mathbf{c}_i^D$ is defined as follows:

$$\mathbf{c}_i^D = [C_i[1], \ldots, C_i[d]]^{\top} \tag{19}$$

Be noted that there may be a repeat in the encrypted readings in $\mathbf{c}_i^B$ and $\mathbf{c}_i^D$ since as mentioned before, the aggregator should save the most recent reported reading from SM_i for the event that it does not transmit a reading due to an insufficient change in the power consumption.

F. BILL COMPUTATION USING DYNAMIC PRICING

In addition to utilizing the CAT readings for energy management and load monitoring, they are also used for the calculation of consumers' bills in case of using dynamic pricing. This section discusses how the EU utilizes the encrypted CAT readings for computing bills.

At every billing interval T_B, the EU computes the bill using b encrypted CAT readings ($\mathbf{c}_i^B$ vector) from every SM_i, $\{1 \leq i \leq |\mathbb{SM}|\}$ as follows.

1) At the termination of every billing interval T_B, the aggregator calculates the billing for the encrypted aggregated readings $C_{agg}^b[i]$ for each SM_i.

$$C_{agg}^b[i] = \prod_{t=1}^{b} C_i[t] \mod n^2 \tag{20}$$

2) For every billing computation, the aggregator also utilizes the private key x_{agg} to compute the signature. This is shown in this formula.

$$\sigma_{agg}^b[i] = x_{agg} H\left(C_{agg}^b[i] \| T_t\right) \tag{21}$$

3) The aggregator sends a message to the EU which contains a tuple of the encrypted aggregated reading, timestamp, and a signature. The tuple is as follows.

$$C_{agg}^b[i] \| T_t \| \sigma_{agg}^b[i] \tag{22}$$

4) To recover the aggregated reading for billing, the EU first checks whether the timestamp is fresh or not, and then also validates the signature upon receiving the message from the aggregator through

$$\hat{e}\left(\sigma_{agg}^b[i], V\right) \stackrel{?}{=} \hat{e}\left(H\left(C_{agg}^b[i] \| T_t\right), Y_{gw}\right) \tag{23}$$

Then, the EU decrypts the aggregated reading for billing for SM_i $C_{agg}^b[i]$ using the secret key (λ, μ) by performing the following operations.

$$\begin{aligned}D\left(C_{agg}^b[i]\right) &= L\left(C_{agg}^b[i]^{\lambda} \bmod n^2\right) \cdot \mu \bmod n \\ &= \sum_{t=1}^{b} m_i[t])\end{aligned} \tag{24}$$

After executing the aforementioned steps, the result $(\sum_{t=1}^{b} m_i[t])$ is the sum of the CAT consumption readings of each SM individually at the end of each billing interval T_B. Hence, our model has attain the functionality requirement (F2) of computing bills of each consumer.

G. POWER THEFT DETECTION

This section explains the training process of the detection model and its architecture. Furthermore, it explains how the EU can identify malicious consumers while protecting their privacy without accessing the plaintext CAT readings.

1) POWER THEFT DETECTOR

In AMI networks, recent research results show that power theft detectors based on machine learning outperform those based on state estimation and game theory [22]. In particular, deep learning-based machine learning detectors, e.g., RNN and CNN [19], [44], are more accurate in identifying power thefts as opposed to shallow detectors, e.g., support vector machine and decision tree, [16], [19], [20], [44], [50]. Furthermore, the power theft detector can be either generic, i.e., it can be utilized for all consumers, or customer-specific, i.e., a tailored detector is trained for each consumer. Therefore, as opposed to general detectors, customer-specific detectors cannot be employed to detect false-reading attacks until enough historical power consumption readings for each consumer are collected which may be a challenge, especially for new consumers. Additionally, customized detectors are susceptible to contamination attacks, in which new consumers initially send false readings, and in this case, the malicious consumers will not be detected if they continue to report false data [22].

The following characteristics of our detector will be based on the discussion above. It will be a generic detector that can be utilized for any consumer (old or new) since it will be trained on all consumers' CAT power consumption readings using a deep learning model. By using deep learning, our detector can recognize correlations in the CAT readings. Additionally, a hybrid two-stage deep learning architecture that comprises CNN preceding a GRU and FFN layers is considered when designing our detector to improve its detection performance. In our detector, the logic behind using the sequence of CNN and GRU is that the most distinctive features in the input CAT readings can be extracted by CNN while the time-correlations within the extracted features can be captured by GRU, resulting in high detection performance. It is note worthy mentioning that the first layer, in our hybrid detector, is a convolution layer where there are a set of max pooling layers and independent filters. Moving each filter over the input and doing dot product operations between the input and filter are how the convolution process is carried out. Homomorphic encryption help us perform the dot product of the encrypted data, hence our model can be evaluated to protect consumers' privacy.

2) PRIVACY-PRESERVING EVALUATION OF POWER THEFT DETECTOR

Our approach leverages the homomorphic encryption's ability to perform dot product operations on encrypted data. Hence, our model is evaluated using the encrypted CAT readings to protect the consumers' privacy. In our model architecture, only the first layer operations are performed using the encrypted data. The result of these operations are used by the EU to resume the subsequent layer's operations. In homomorphic, given that the encrypted message m is $E(m)$, and when it is raised to the power x, it results in the encryption of m multiplied by x as indicated in the following formula.

$$E(m)^x = g^{x \cdot m} \cdot \left(r^x\right)^N \bmod N^2 = E(x \cdot m) \tag{25}$$

Generally, the main operation in the convolutional layer in a neural network's CNN architecture is the dot product which is represented by $\mathbf{z} = \boldsymbol{m}\mathbf{W}$, where $\boldsymbol{m}$ is the input vector and $\mathbf{W}$ is the weight matrix. In our CNN-GRU model, given f $1-d$ filters in the first convolutional layer and d features (input neurons), the dimension of the first layer weight matrix is represented as $(d \times f)$. In our paradigm, the input vector is multiplied by $\boldsymbol{W}$ to perform the dot product operation ($\boldsymbol{m}\mathbf{W}$) of the first layer, yielding to f components which are corresponding to f dot product operations between each filter in $\boldsymbol{W}$ and the input. Thus, in order to protect the privacy of the consumers, the homomorphic encryption's ability to compute the dot product operations on encrypted data is used in the first convolutional layer and get the result that is:

$$\boldsymbol{m}_i \boldsymbol{W}, \tag{26}$$

where the input $\boldsymbol{m}_i$ represents the SM_i's CAT readings for the period T_D, and it can be expressed by $[\boldsymbol{m}_i[1], \boldsymbol{m}_i[2], \ldots, \boldsymbol{m}_i[d]]$.

The EU sends the power theft detector's parameters to the aggregator so that the aggregator can perform the model operations and then sends the encrypted results to the EU. The encrypted results are then sent to the EU by the aggregator at the end of each detection interval T_D so that the EU can decrypt these results by using the homomorphic decryption key to be able to evaluate the power theft detector. This process is done for each SM_i to identify malicious and honest consumers. $[\boldsymbol{w_1}^\top, \boldsymbol{w_2}^\top, \ldots, \boldsymbol{w_b}^\top]$ represents the f columns of $\boldsymbol{W}$, where $\boldsymbol{w}_j$ is the j_{th} column of $\boldsymbol{W}$, and $\boldsymbol{w}_j = [\boldsymbol{w}_j[1], \boldsymbol{w}_j[2], \ldots, \boldsymbol{w}_j[d]]^\top \in \mathbb{Z}_q^d$. The following is how the detection model is evaluated.

- Step 1: The encrypted dot product between each column of $\boldsymbol{W}$ and the ciphertexts of SM_i $\mathbf{c}_i^D$ (encrypted CAT readings for T_D) is computed by the aggregator by the end of each T_D by carrying out the following steps.

$$C_{agg}^d[i] = \left[\sum_{t=1}^{d} m_i[t] \times \boldsymbol{w}_j[t]\right] = \prod_{t=1}^{d} C_i[t]^{\boldsymbol{w}_j[t]} \tag{27}$$

  where $C_{agg}^d[i]$ is the encrypted dot product results.
- Step 2: The signature of each encrypted inner product results for every SM_i, i.e., $C_{agg}^d[i]$ is calculated through the aggregator's private key x_{agg}.

$$\sigma_{agg}^d[i] = x_{agg} H\left(C_{agg}^d[i] \| T_t\right) \tag{28}$$

- Step 3: The EU receives a message containing the encrypted dot product results and its signature sent by the aggregator. The following tuple should be included in the message.

$$C_{agg}^d[i] \| T_t \| \sigma_{agg}^d[i] \tag{29}$$

- To recover the dot product results, the EU first checks whether the timestamp is fresh or not and also validates the signature upon receiving the message from the aggregator by verifying the following.

$$\hat{e}\left(\sigma^{d}_{agg}[i], P\right) \stackrel{?}{=} \hat{e}\left(H\left(C^{d}_{agg}[i] \| T_t\right), Y_{agg}\right) \quad (30)$$

Then, given the homomorphic decryption key (λ, μ) and the encrypted dot product results from the aggregator $C^{d}_{agg}[i]$ for each SM_i, the EU decrypts the first convolutional layer's output by performing the following steps.

$$D\left(C^{d}_{agg}[i]\right) = L\left(C^{d}_{agg}[i]^{\lambda} \bmod n^2\right) \cdot \mu \bmod n \quad (31)$$

$$= \sum_{t=1}^{d} \boldsymbol{w}_j[t]\boldsymbol{m}_i[t], j = 1, 2, \ldots, b \quad (32)$$

- The EU continues running the power theft detector by having the first hidden layer's output which is the next layer's input, and operation is further performed in the subsequent hidden layers until the final output layer's calculation is completed and classification is done.

Therefore, the EU can evaluate our CNN-GRU-based detector securely at the end of each T_D without being able to learn the CAT readings to protect the consumers' privacy. Hence, the functionality requirement (F3) of detecting power thefts while preserving privacy can be achieved by our scheme.

In the literature, the HE is used in one of two approaches, called separation of knowledge [51], [52], [53] and masking [54]. In the first approach, the EU knows the HE's private key but it cannot access the ciphertexts of the individual readings. Specifically, a non-colluding entity (i.e., the aggregator) aggregates the consumption readings and send the ciphertext of the aggregated readings to the EU to decrypt and know the aggregated reading without being able to learn the individual readings. To protect the scheme against external eavesdroppers, all the communications between the smart meters and the aggregators are secured using symmetric-key encryption. For the masking approach, it does not need a non-colluding entity. It executes a secret sharing technique by the smart meters to share secret masks, and then the meters mask their readings in such a way that by aggregating the encrypted readings, the total aggregated reading can be computed because the masks added by the meters nullify. In this case, if the EU accesses an encrypted reading, it can only compute a masked reading and it cannot de-mask the reading because it does not know the secret masks. In this paper, we prefer the first approach to avoid the overhead of the secret sharing technique and because some computations are done by the aggregator and other computations are done by the EU.

VII. RESULTS AND DISCUSSION

The performance of the power theft detector is evaluated and the computation and communication overheads are measured.

TABLE 4. Performance metrics of power theft detector.

Metric	Definition
Detection rate (DR)	$\frac{TP}{TP+FN}$
False alarm (FA)	$\frac{FP}{TN+FP}$
Highest difference (HD)	$DR - FA$
Accuracy (Acc)	$\frac{(TP+TN)}{TN+TP+FP+FN}$

A. POWER THEFT DETECTION

1) PERFORMANCE METRICS

TP, *TN*, *FP*, and *FN* are true positive, true negative, false positive, and false negative, respectively. Table. 4 presents the performance metrics used to assess our detector in terms of accuracy (Acc), detection rate (DR), false alarm (FA), and highest difference (HD). The detection rate measures the proportion of fraudulent consumers identified correctly, while the false acceptance rate gauges the portion of honest customers mistakenly categorized as fraudulent. The highest difference is the difference between the detection rate and the false alarm rate. The accuracy is the percentage of honest/fraudulent customers correctly identified as honest/fraudulent, respectively. The model's performance is better when *FA* is low, and *HD*, *Acc*, and *DR* are high. Because there is no current proposal for CAT AMI we can compare to it in the performance evaluations, we compare our CNN_GRU detector to a CNN detector because it is widely used in the literature in case of periodic transmission AMI [16], [44], [55], [56], [57], [58], [59].

2) RESULTS AND DISCUSSION

In this subsection, we first train a power theft detector using a CNN model because it is widely used in the literature in PT AMI, and we consider this model the baseline. Then, we train a power theft detector using the hybrid architecture (CNN & GRU model) by adding a GRU model after the fully connected layer of the CNN. We train the two detectors using 144 CAT readings reported by the consumers' smart meters. To conduct a thorough investigation, the power theft detectors are trained on both malicious and benign samples using the dataset discussed in Section IV. $\ell 2-$regularization is used while training the model to prevent over-fitting. Moreover, Based on a validation dataset, the hyper-parameters of the detectors are modified using the hyperopt tool [60] to fine-tune the quantity of filters and units in the CNN and GRU layers, respectively, and select learning rate, batch size, and activation function for each layer. Table 5 shows the optimum hyper-parameter for the model. Next, the test dataset is used to evaluate our models. Python3 libraries (e.g., Keras [61] and Numpy) are used to train our model. These libraries were installed on high performance clusters of Tennessee Technological University with an NVIDIA Tesla K80 GPU.

TABLE 5. Hybrid CNN-GRU-based detector's optimal hyper-parameters.

Architecture	Hyper-parameters		
	Layer	Number of units	AF
CNN-GRU	Input	144	Linear
	Conv1D	64	Tanh
	Conv1D	128	Tanh
	MaxPooling1D	2	–
	GRU	32	Tanh
	Dense	512	Elu
	Dense	64	Relu
	Dense	128	Relu
	Output	2	Softmax
	Output	2	Softmax

TABLE 6. Performance comparison between various detectors.

Architecture	Metrics			
	ACC	DR	FA	HD
CNN	93.85	93.98	6.28	87.7
CNN+GRU	97.14	97.45	3.17	94.28

Table 6 reveals the evaluation results of the CNN-GRU model and the CNN model. Our model has a higher accuracy and *DR*, 97.14% and 97.45%, respectively, in comparison to the CNN-based model which has 93.85% accuracy and 93.98% *DR*. Moreover, our model attains a higher *HD* (94.28%) compared to the *HD* of the CNN model (87.7%) as shown in Table 6. Consequently, it can be concluded that the detector with a hybrid of CNN & GRU offers the best performance due to its CNN layers' capability to learn distinctive features from the inputted CAT readings and its GRU layers' ability to capture the long term correlations among features.

Furthermore, Our model is applicable to all consumers without the need for collecting prior data from individual consumers, so it is resilient against contamination attacks. Figure 7 reveals the Receiver Operating Characteristics (ROC) curves of the detectors, with the area under curve (AUC) serving as a measure for accuracy. It is evident from the results presented in the figure that our model offers superior performance compared to the CNN model.

B. COMMUNICATION AND COMPUTATION OVERHEAD

Our approach is implemented on Python Charm library [62] using a 1GB RAM, 1.2GHz Processor, and Raspberry Pi 3. 512 bytes (2048 bits) are used for the primes' length p and q in the Paillier Homomorphic Cryptosystem. It is important to note that, for security reasons, it is recommended the primes' length p and q should be at least 1024 bits [63], [64].

1) COMPUTATION OVERHEAD

It is the amount of time it takes for each entity in the network (the EU, the aggregator, and the SMs) to do the computations needed by our scheme. When there is enough change in the consumption and the smart meter needs to transmit an encrypted CAT reading, this requires two exponentiation and one multiplication operations over $\mathbb{Z}_n^2$ to calculate the ciphertext, and one multiplication operation for the signature. In each time slot T_t, after the ciphertexts are received from w SMs ($w \leq |\mathbb{SM}|$), the aggregator initially executes w pairing operations for the batch verification process to verify the integrity and authenticity of the consumption readings. Furthermore, it should aggregate the readings of different SMs by performing $w-1$ multiplication operations in $\mathbb{Z}_n^2$ for load monitoring and energy management.

The aggregator performs $b-1$ multiplication operations in $\mathbb{Z}_n^2$ for billing purposes for each SM or a total of ($|\mathbb{SM}| \times b-1$) multiplication operations for all SMs at the end of every billing interval T_B, after having b encrypted CAT readings ($\mathbf{c}_i^B$ vector) from each SM_i, $\{1 \leq i \leq |\mathbb{SM}|\}$.

For privacy-preserving power theft detector evaluation, given that the number of filters in the detector's first hidden layer is 64, the number of CAT readings is 144, and the kernel size for each filter is 13, at the end of every power theft detection interval T_D and after receiving d encrypted CAT readings ($\mathbf{c}_i^D$ vector) from each SM_i, $\{1 \leq i \leq |\mathbb{SM}|\}$, the aggregator needs to perform 1716 multiplication operations and 1584 addition operations in $\mathbb{Z}_n^2$ for power theft detection for each SM for each filter. For simplicity, a total of $132 = (144 - 13 + 1)$ dot product operations are needed, where each dot product operation requires 13 multiplication and 12 addition operations for a total of $1716 = 132 \times 13$ multiplication operations, where 132 is coming from $(144-13+1)$ and $1584 = 132 \times 12$ addition operations. Moreover, the aggregator computes the signature through a multiplication operation in $\mathbb{U}$ for the purpose of load monitoring, billing, and power theft detection.

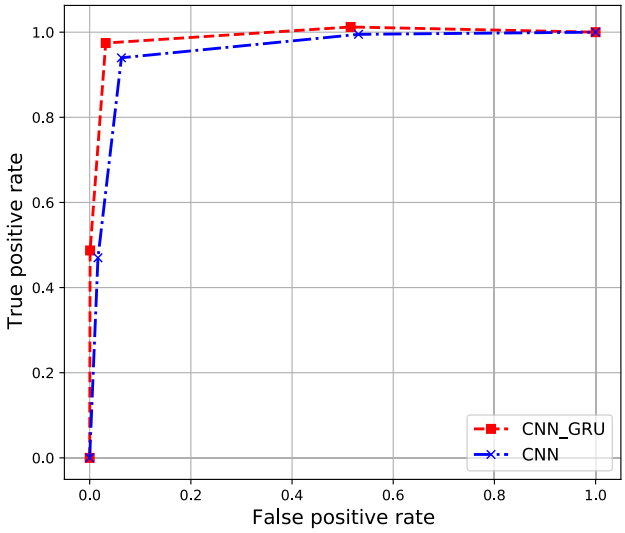

FIGURE 7. Comparison between the ROC curves of the CNN and CNN_GRU power theft detectors.

The EU performs one pairing operation to verify the encrypted aggregated data from the aggregator, and then it performs one exponentiation operation in $\mathbb{Z}_n^2$ to decrypt each aggregated ciphertext. Therefore, the EU performs one exponentiation operation for load monitoring in each time slot T_t, $|\mathbb{SM}|$ exponentiation operations for billing computation for all SMs at the termination of every billing interval T_B, and $|\mathbb{SM}| \times 8448$ exponentiation operations for power theft detection for all SMs at the termination of every billing interval T_D.

2) COMMUNICATION OVERHEAD

It is the amount of data transmitted between network entities, i.e., SM-to-aggregator and aggregator-to-EU. The communication overhead of our CAT approach is compared to the periodic transmission (PT). PT AMI allows periodic transmission of encrypted readings even if there is no enough change in the current reading comparing to the last reading, while in CAT AMI, smart meters report ciphertext of consumption readings to aggregator only when the change in the consumption comparing to the last reading exceeds a certain threshold, 10% in this paper. Since 512 bytes Paillier cryptosystem is used, the sizes of an encrypted reading, timestamp and signature are is 512 byte, 4, and 64 bytes, respectively. Therefore, given 10 minutes transmission rate (144 readings per day), the communication overhead among smart meters and the aggregator is 83,520 (580 $\times$ 144) bytes per day for each SM in case of transmitting the consumers' power consumption readings periodically compared to 62,640 bytes using our scheme. Therefore, there is about 25% saving gained in the communication overhead (bandwidth) as a result of using the CAT transmission of power readings. As can be seen from these results, the communication overhead incurred in our CAT AMI approach is superior to using PT AMI even with preserving privacy.

C. SECURITY AND PRIVACY ANALYSIS

Our scheme is capable of achieving the desired security/privacy requirements need to thwart the attacks discussed in Section III-B.

1) SECURE DETECTION OF POWER THEFT

The outcomes presented in subsection VII-A illustrate the effectiveness of our power theft detection system in identifying attempts made by dishonest consumers to steal power. To ensure the secure evaluation of our power theft detector, each SM encrypts its readings using homomorphic encryption. This encryption allows the EU to compute the output of the first layer of the detector without gaining knowledge of the individual meter readings. The resulting output is then fed into subsequent layers of the detector to determine the classification result. Furthermore, the EU employs the same encrypted readings for monitoring, billing, and evaluating the detector. This approach prevents deceptive behavior from a consumer who might try to bypass the detector by submitting two different sets of readings: one for billing and monitoring purposes, and another for theft detection. As a result, our scheme effectively safeguards against such deceptive actions, ensuring that it meets the security requirements for privacy-preserving theft detection.

2) CONSUMERS' PRIVACY PRESERVATION

To ensure consumer privacy, the CAT readings of the consumers are encrypted in such a way that no entity, including the EU, can gain access to the individual readings. Moreover, even if the same reading is repeated at different times, the encrypted ciphertext appears different due to the utilization of a unique random number during each encryption process. This effectively thwarts any attempts at traffic analysis attacks. The utilization of a random number, denoted as r, must be done only once. Reusing the same random number can lead to a vulnerability where the difference between two readings, denoted as m_1 and m_2, can be obtained by dividing their respective ciphertexts. By solving the equation $g^{m_1} \cdot r^n / g^{m_2} \cdot r^n = g^{m_1 - m_2}$, one can deduce the value of $m_1 - m_2$. Consequently, if one reading is known, the other reading can be obtained. For the EU to learn the power consumption reading of a specific consumer, collusion with ($|\mathbb{SM}|$-1) consumers is required. This collusion involves subtracting the total power consumption of the colluding smart meters (SMs) from the total power consumption known to the EU. However, this type of attack becomes infeasible when the number of SMs in an AMI network is sufficiently large. As a result, our scheme ensures that no entity within the network, including the EU, is granted access to the consumers' consumption readings, satisfying the requirement for maintaining privacy in the system.

3) CONSUMERS' BILLS AND TOTAL POWER CONSUMPTION CONFIDENTIALITY

Once the encrypted cumulative power consumption of an AMI is calculated by the aggregator from the encrypted CAT readings received from smart meters, it is the responsibility of the aggregator to transmit this ciphertext to the EU for load monitoring purposes. In the event that attackers intercept the encrypted readings, they will gain no knowledge about the individual readings nor the overall power consumption of the AMI. This is due to the complex decryption process, which involves a private key exclusively known to the EU. Only the EU possesses this key, allowing it to decrypt the homomorphic ciphertext and obtain the aggregated power consumption reading. Additionally, the EU is the sole entity capable of computing the billing information for each consumer. This is achieved by employing a secret key that is exclusively known to the EU. As a result, the EU possesses the authority to access both the overall consumption data of consumers for load management purposes and the individual billing details of each consumer.

VIII. CONCLUSION AND FUTURE WORKS

This paper proposes a deep-learning solution for power theft detection in CAT AMI networks while preserving consumers'

privacy. Specifically, our proposal enables the EU to detect power theft, compute bills using dynamic pricing, and perform load monitoring and energy management, without being able to learn the individual readings of the smart meters. Disclosing the consumers' readings jeopardizes consumers' privacy due to the fact that these readings can reveal sensitive information about consumers' lifestyles, e.g., their presence or absence, the appliances they use, etc. In order to obtain benign data for the CAT AMI, a real power consumption readings dataset is processed, and to generate malicious samples, a novel collection of attacks specifically designed for CAT AMI are proposed and implemented on the benign dataset. Our proposal leverages the ability of the Pailer cryptography to perform dot product operation over encrypted data in addition to privacy-preserving data aggregation. The do product operations are used to evaluate the detector without revealing the plaintext input readings while the data aggregation is used for billing, load monitoring, and energy management. Through extensive experiments, our approach was proven to accurately detect fraudulent consumers without compromising consumers' privacy with reasonable overhead.

For future research directions, in smart grid net-metering systems, renewable energy generators, like solar panels and wind turbines, are installed at homes to generate energy. In this case, houses have batteries that may need to charge from the grid (buy electricity) or inject power to the grid (sell energy). In this system, the smart meters report the difference between the energy consumption and the amount of injected energy. Positive readings indicate that the house consumed energy from the grid, while negative readings indicate that the house injected power to the grid. In our future work, we will investigate electricity theft in this system.

REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[2] O. B. J. Rabie, P. K. Balachandran, M. Khojah, and S. Selvarajan, "A proficient ZESO-DRKFC model for smart grid SCADA security," *Electronics*, vol. 11, no. 24, p. 4144, Dec. 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/24/4144

[3] S. Shitharth, K. M. Prasad, K. Sangeetha, P. R. Kshirsagar, T. S. Babu, and H. H. Alhelou, "An enriched RPCO-BCNN mechanisms for attack detection and classification in SCADA systems," *IEEE Access*, vol. 9, pp. 156297–156312, 2021.

[4] 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.

[5] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.

[6] 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. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7.

[7] M. I. Ibrahem, M. Nabil, M. M. Fouda, M. 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.

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

[9] 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.

[10] A. Alsharif, M. Nabil, M. Mahmoud, and M. Abdallah, "Privacy-preserving collection of power consumption data for enhanced AMI networks," in *Proc. 25th Int. Conf. Telecommun. (ICT)*, Jun. 2018, pp. 196–201.

[11] 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. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2021, pp. 1–7.

[12] (Mar. 2020). *Electricity Thefts Surge in Bad Times*. [Online]. Available: https://www.usatoday30.usatoday.com/money/industries/energy/2009-03-16-electrcity-thefts.html

[13] 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.

[14] 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.

[15] S. A. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 883–894, Mar. 2016.

[16] Z. Zheng, Y. Yang, X. Niu, H. 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.

[17] 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)*, Dec. 2014, pp. 1–6.

[18] 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.

[19] 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. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 272–279.

[20] 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.

[21] M. Joudaki, P. T. Zadeh, H. R. Olfati, and S. Deris, "A survey on deep learning methods for security and privacy in smart grid," in *Proc. 15th Int. Conf. Protection Autom. Power Syst. (IPAPS)*, Dec. 2020, pp. 153–159.

[22] 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. 24th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 740–745.

[23] M. I. Ibrahem, M. M. E. A. Mahmoud, F. Alsolami, W. Alasmary, A. S. A. AL-Ghamdi, and X. Shen, "Electricity-theft detection for change-and-transmit advanced metering infrastructure," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25565–25580, Dec. 2022.

[24] K. Gajowniczek, T. Ząbkowski, and M. Sodenkamp, "Revealing household characteristics from electricity meter data with grade analysis and machine learning algorithms," *Appl. Sci.*, vol. 8, no. 9, p. 1654, Sep. 2018.

[25] K. Weaver, *A Perspective on How Smart Meters Invade Individual Privacy*. Hoboken, NJ, USA: Sky Vision Solution Press, 2014.

[26] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters using deep reinforcement learning," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT-Eur.)*, Oct. 2020, pp. 929–933.

[27] B. C. Gajarla, A. V. Rebba, K. S. Kakathota, M. Kummari, and S. Shitharth, "Handling tactful data in cloud using PKG encryption technique," in *Proc. 4th Smart Cities Symp. (SCS)*, Nov. 2021, pp. 338–343, doi: 10.1049/icp.2022.0366.

[28] M. S. Yoosuf, C. Muralidharan, S. Shitharth, M. Alghamdi, M. Maray, and O. B. J. Rabie, "FogDedupe: A fog-centric deduplication approach using multi-key homomorphic encryption technique," *J. Sensors*, vol. 2022, pp. 1–16, Aug. 2022.

[29] Kolter. (2020). *Residential Energy Disaggregation Dataset (REDD)*. [Online]. Available: http://traces.cs.umass.edu/index.php/Smart/Smart

[30] G. Eibl and D. Engel, "Influence of data granularity on smart meter privacy," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 930–939, Mar. 2015.
[31] J. M. Junior, J. P. C. L. D. da Costa, C. C. R. Garcez, R. D. O. de Oliveira Albuquerque, A. Arancibia, L. Weichenberger, F. L. L. D. de Mendonça, G. D. Galdo, and R. T. D. S. de Sousa Jr., "Data security and trading framework for smart grids in neighborhood area networks," *Sensors*, vol. 20, no. 5, p. 1337, Feb. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/5/1337
[32] I. Dataset. (Sep. 2020). *Irish Social Science Data Archive*. [Online]. Available: http://www.ucd.ie/issda/data/commissionforenergyregulationcer
[33] S. Dataset. (Sep. 2020). *State Grid Corporation of China*. [Online]. Available: http://www.sgcc.com.cn/
[34] C. Richardson, N. Race, and P. Smith, "A privacy preserving approach to energy theft detection in smart grids," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2016, pp. 1–4.
[35] M. Wen, R. Xie, K. Lu, L. Wang, and K. Zhang, "FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6069–6080, Apr. 2022.
[36] R. Pal, P. Hui, and V. Prasanna, "Privacy engineering for the smart micro-grid," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 5, pp. 965–980, May 2019.
[37] K. Samarakoon, J. Ekanayake, and N. Jenkins, "Reporting available demand response," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1842–1851, Dec. 2013.
[38] 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.
[39] S. Werner and J. Lunden, "Event-triggered real-time metering in smart grids," in *Proc. 23rd Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2015, pp. 2701–2705.
[40] J. Lundén 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.
[41] 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. 2017.
[42] M. M. Badr, M. M. E. A. Mahmoud, Y. Fang, M. Abdulaal, A. J. Aljohani, W. Alasmary, and M. I. Ibrahem, "Privacy-preserving and communication-efficient energy prediction scheme based on federated learning for smart grids," *IEEE Internet Things J.*, vol. 10, no. 9, pp. 7719–7736, May 2023.
[43] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7659–7669, Oct. 2019.
[44] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary, and E. Serpedin, "PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96334–96348, 2019.
[45] Kolter. *Residential Energy Disaggregation Dataset (REDD)*. Accessed: Jul. 2, 2023. [Online]. Available: http://traces.cs.umass.edu/index.php/Smart/Smart
[46] H. He, Y. Bai, E. A. Garcia, and S. Li, "ADASYN: Adaptive synthetic sampling approach for imbalanced learning," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IEEE World Congr. Comput. Intell.)*, Jun. 2008, pp. 1322–1328.
[47] A. Stergiou and R. Poppe, "AdaPool: Exponential adaptive pooling for information-retaining downsampling," *IEEE Trans. Image Process.*, vol. 32, pp. 251–266, 2023.
[48] D. Scherer, A. Müller, and S. Behnke, "Evaluation of pooling operations in convolutional architectures for object recognition," in *Artificial Neural Networks ICANN 2010*, K. Diamantaras, W. Duch, and L. S. Iliadis, Eds. Berlin, Germany: Springer, 2010, pp. 92–101.
[49] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology EUROCRYPT*, J. Stern, Ed. Berlin, Germany: Springer, 1999, pp. 223–238.
[50] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.
[51] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
[52] Y. Chen, J. Martínez-Ortega, P. Castillejo, and L. López, "A homomorphic-based multiple data aggregation scheme for smart grid," *IEEE Sensors J.*, vol. 19, no. 10, pp. 3921–3929, May 2019.
[53] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2703–2713, Mar. 2017.
[54] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Applied Cryptography and Network Security*, F. Bao, P. Samarati, and J. Zhou, Eds. Berlin, Germany: Springer, 2012, pp. 561–577.
[55] L. Zhu, W. Wen, J. Li, C. Zhang, B. Zhou, and Z. Shuai, "Deep active learning-enabled cost-effective electricity theft detection in smart grids," *IEEE Trans. Ind. Informat.*, early access, Mar. 23, 2023, doi: 10.1109/TII.2023.3249212.
[56] J. Li, W. Liao, R. Yang, and Z. Chen, "A data augmentation method for distributed photovoltaic electricity theft using Wasserstein generative adversarial network," in *Proc. IEEE 5th Conf. Energy Internet Energy Syst. Integr. (EI)*, Oct. 2021, pp. 3132–3137.
[57] Y. Zhou, X. Zhang, Y. Tang, Z. Mu, X. Shao, Y. Li, and Q. Cai, "Convolutional neural network and data augmentation method for electricity theft detection," in *Proc. IEEE/IAS Ind. Commercial Power Syst. Asia (I&CPS Asia)*, Jul. 2021, pp. 1525–1530.
[58] M. J. Abdulaal, M. I. Ibrahem, M. Mahmoud, S. A. Bello, A. J. Aljohani, A. H. Milyani, and A. M. Abusorrah, "DRFD: Deep learning-based real-time and fast detection of false readings in AMI," in *Proc. SoutheastCon*, Mar. 2022, pp. 682–689.
[59] 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.
[60] J. Bergstra, B. Komer, C. Eliasmith, D. Yamins, and D. D. Cox, "Hyperopt: A Python library for model selection and hyperparameter optimization," *Comput. Sci. Discovery*, vol. 8, no. 1, Jul. 2015, Art. no. 014008, doi: 10.1088/1749-4699/8/1/014008.
[61] F. Chollet. (2015). *Keras*. [Online]. Available: https://github.com/fchollet/keras
[62] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, Jun. 2013.
[63] S. S. Reddy, S. Sinha, and W. Zhang, "Design and analysis of RSA and Paillier homomorphic cryptosystems using PSO-based evolutionary computation," *IEEE Trans. Comput.*, vol. 72, no. 7, pp. 1886–1900, Jul. 2023.
[64] W. Wang, Z. Chen, and X. Huang, "Accelerating leveled fully homomorphic encryption using GPU," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 2800–2803.

MOHAMMED J. ABDULAAL received the B.Eng. degree in mechatronic engineering from The University of Manchester, U.K., in 2012, the M.Sc. degree in mechanical engineering from King Abdullah University for Science and Technology, in 2014, and the Ph.D. degree from the School of Electrical and Electronic Engineering, The University of Manchester, in 2019. His Ph.D. research involved design and implementation of a low-level electroencephalography recognition system and brain–computer Interface. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, King Abdulaziz University, Saudi Arabia. His research interests include signal processing and machine learning of biomedical systems, Hajj research, traffic control systems, cybersecurity, and various image processing applications.

MOHAMED M. E. A. MAHMOUD (Senior Member, IEEE) received the Ph.D. degree from the University of Waterloo, in April 2011. From May 2011 to May 2012, he worked as a Postdoctoral Fellow with the Broadband Communications Research Group, University of Waterloo. From August 2012 to July 2013, he worked as a Visiting Scholar with the University of Waterloo and a Postdoctoral Fellow with Ryerson University. He is currently a Professor with the Department Electrical and Computer Engineering, Tennessee Technological University, USA. He is the author of more than 120 articles and the PI for more than U.S. $2 million of research fund. His research interests include security and privacy preserving schemes for smart power grid, smart healthcare, and smart transportation; applied machine learning; and adversarial machine learning. He has received several prestigious awards, such as the NSERC-PDF (Canada), the U.S. Scholar Fulbright (USA), and the Best Paper Award from IEEE WCNC, ICC, and SmartNets. He served as a technical program committee member for several IEEE conferences and a reviewer for several journals and conferences. He also serves as an Associate Editor for IEEE INTERNET OF THINGS JOURNAL.

SAHEED A. BELLO received the bachelor's degree from Obafemi Awolowo University, Ile-Ife, Nigeria. He is currently pursuing the degree with the Department of Electrical and Computer Engineering, King Abdulaziz University, Saudi Arabia. His research interests include computer vision and machine learning.

JUNAID KHALID received the B.S. degree in electrical engineering from the University of South Asia, Lahore, Pakistan, in 2015. He is currently pursuing the M.S. degree with the Department of Electrical and Computer Engineering, King Abdulaziz University, Saudi Arabia. He is also a Graduate Research Assistant with the Department of Electrical and Computer Engineering, King Abdulaziz University. His research interests include sustainable energy systems, optimization of power systems, and smart grids.

ABDULAH JEZA ALJOHANI received the B.Sc. (Eng.) degree in electronics and communication engineering from King Abdulaziz University, in 2006, and the M.Sc. and Ph.D. degrees in wireless communication from the University of Southampton, Southampton, U.K., in 2010 and 2016, respectively. He is currently a Research and Innovation Consultant with the Communications and Information Technology Commission (CITC), and an Associate Professor with the Department of Electrical and Computer Engineering, King Abdulaziz University. His research interests include channel coding, cooperative communications, free-space optical communication, and MIMO systems.

AHMAD H. MILYANI received the B.Sc. (Hons.) and M.Sc. degrees in electrical and computer engineering from Purdue University, in 2011 and 2013, respectively, and the Ph.D. degree in electrical engineering from the University of Washington, in 2019. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include power systems operation and optimization, renewable and sustainable energy, power electronics, electric machines, electric vehicles, and the applications of computational intelligence.

ABDULLAH M. ABUSORRAH (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Nottingham, U.K., in 2007. He is currently a Professor with the Department of Electrical and Computer Engineering, King Abdulaziz University, where he is currently the Head of the Center for Renewable Energy and Power Systems. His research interests include renewable energy, smart grid, the Internet of Things (IoT), and system analysis.

MOHAMED I. IBRAHEM received the B.S. and M.S. degrees in electrical engineering (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 Technological University, USA, in 2021. He is currently an Assistant Professor with the School of Computer and Cyber Sciences, Augusta University, USA. He also holds the position of a Lecturer Assistant with Benha University. His research interests include machine learning, cryptography and network security, and privacy-preserving schemes for smart grid communication and AMI networks. He received the Eminence Award for the Doctor of Philosophy Best Paper from Tennessee Technological University.