IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 September 2024, accepted 4 October 2024, date of publication 10 October 2024, date of current version 28 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3478068

RESEARCH ARTICLE

Efficient and Privacy-Preserving ConvLSTM-Based Detection of Electricity Theft Cyber-Attacks in Smart Grids

JOHNSON ANIN[1], MUHAMMAD JAHANZEB KHAN[2], OMAR ABDELSALAM[3], MAHMOUD NABIL[4], (Senior Member, IEEE), FEI HU[1], (Member, IEEE), AND AHMAD ALSHARIF[2,5], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL 35487, USA
[2]Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487, USA
[3]Department of Computer Science, Tennessee Tech University, Cookeville, TN 35405, USA
[4]Electrical and Computer Engineering, University of North Carolina A&T, Greensboro, NC 27411, USA
[5]Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Banha 13511, Egypt

Corresponding author: Ahmad Alsharif (ahmad.alsharif@ua.edu)

This work was supported by the U.S. National Science Foundation (NSF) under Grant 2244371.

ABSTRACT In Advanced Metering Infrastructure (AMI) networks, Smart Meters (SMs), are installed at consumers' houses, provide electric utilities with fine-grained power consumption data necessary for accurate billing, load monitoring, and energy management. However, utility companies are still subjected to electricity theft cyber-attacks in which fraudulent consumers may manipulate their reported readings and hence reduce their bills. Several ML-based electricity theft detectors have been proposed in the literature, however, they either do not capture well the deeper periodicity and temporal features in energy consumption data or violate consumers' privacy by running these models over unencrypted power consumption data. To address these challenges, we propose in this paper a Conv-LSTM-based detector that integrates a 2-D Convolutional Neural Network (CNN) model with a Long Short-Term Memory (LSTM) network to significantly improve the model's functionality and detection accuracy, specifically addressing the inherent periodicity and temporal dependencies in electricity consumption data. Moreover, to run the proposed model over encrypted 2D data and preserve consumers' privacy, we designed a novel lightweight Inner Product Functional Encryption (IPFE) scheme that allows SMs to send their encrypted power consumption data to the Electric Utility (EU) which can securely compute the first feature map of the first convolutional layer of the Conv-LSTM detector while preserving consumer privacy. Our analysis and experiments demonstrate that our scheme is secure and efficiently detecting fraudulent consumers with minimal overhead. In specific, our model achieves a Detection Rate (DR) of 92.95%, a False Alarm Rate (FAR) of 3.68%, and a High Detection (HD) rate of 89.27%, resulting in an overall Accuracy (ACC) of 94.65%. Moreover, our scheme achieves high Precision (PR) at 98.80% and a robust Area Under the Curve (AUC) value of 98.50%. These results highlight the effectiveness of our approach in enhancing both detection accuracy and reliability all while protecting consumers' privacy.

INDEX TERMS Smart grid, privacy preservation, electricity theft cyber-attacks, Conv-LSTM neural networks, functional encryption.

SG	Smart Grid.
AMI	Advanced Metering Infrastructure.
SM	Smart Meter.
EU	Electric Utility.
ML	Machine Learning.
ETD	Electricity Theft Detection.
DL	Deep Learning.
KDC	Key Distribution Center.

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

FFN	Feed Forward Neural Network.
RNN	Recurrent Neural Network.
CNN	Convolutional Neural Network.
LSTM	Long Short-Term Memory.
IPFE	Inner Product Functional Encryption.

I. INTRODUCTION

The power grid experiences electricity losses due to both technical and non-technical factors [1]. Technical losses typically arise during electricity transfer between electrical installations due to several factors including but not limited to conductor resistance, induction of electromagnetic fields, harmonic distortion, and poor earthing. While these losses are inevitable, their mitigation is possible through improved installation practices [2]. On the other hand, predicting or estimating non-technical losses, caused by malicious manipulation of reported power consumption data, poses a significant challenge. This results in inaccurate billing, leading to huge financial and economic negative impacts in many countries worldwide. For instance, recent reports indicate that the annual financial loss due to non-technical loss is about \$6B, \$173M, and \$100M in the United States, the United Kingdom, and Canada respectively [3]. Moreover, a recent study showed that electricity theft and non-technical losses cost utilities \$101.2 billion annually in lost revenue across 138 countries [4]. Electricity theft not only causes economic losses but also results in a disrupted and unstable grid operation that may result in power outages [5]. Therefore, there is a necessity to make the power grid smarter and immune to these attacks.

This necessity drives the evolution towards the Smart Grid (SG), a modern iteration of the power grid that employs cutting-edge technologies, equipment, and controls. This innovation facilitates bidirectional communication among the grid's various grid components, thereby enhancing the reliability of the power grid and enabling the realization of optimal energy management. Figure 1 shows the conceptual architecture of the SG. As shown in the figure, a major component of the SG is Advanced Metering Infrastructure (AMI) networks, where Smart Meters (SMs), installed at consumers' houses, provide utility companies with fine-grained power consumption data. AMI networks not only empower EU with the necessary data to ensure accurate billing and analyze realtime energy consumption data, but also provide consumers with a substantial degree of convenience in managing their energy consumption [6].

However, integrating SMs into the SG system increases its vulnerability to electricity theft cyber-attacks. Malicious customers can exploit system weaknesses and execute various cyber-attacks to manipulate meter readings. One approach involves utilizing reverse engineering techniques to manipulate the firmware and hardware components of smart meters to report incorrect energy consumption readings for reduction in electricity bills. An example of such an incident occurred in 2014, when smart meters in Spain were hacked to

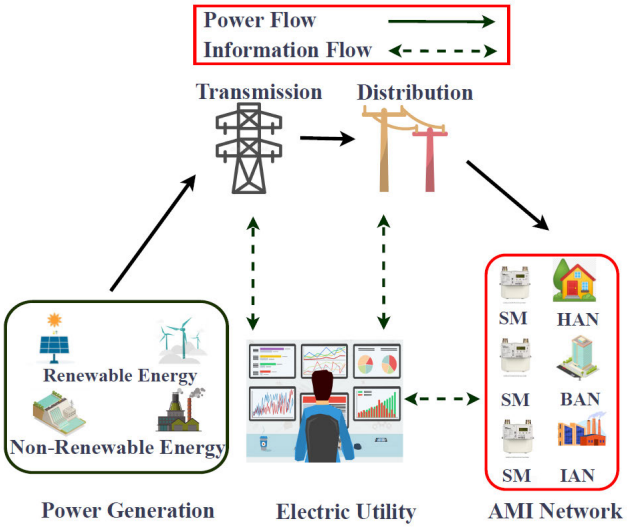

FIGURE 1. The smart grid conceptual architecture.

cut power bills [7]. This fraudulent behavior causes serious financial losses. Beyond financial implications, malicious readings may impact the accuracy of power consumption readings used by the electric utility for grid management. This can potentially lead to grid instability or even blackout in severe cases. A key example is the Ukrainian power grid attack in December 2015, which plunged the country in total darkness during a harsh winter [8].

To detect such fraudulent activities and identify malicious consumers, Machine Learning (ML)-based solutions have been proposed. In these solutions, EUs train ML models over consumers' power consumption data to achieve high detection accuracy of such attacks. However, allowing the EU to continuously access consumers' readings for Electricity Theft Detection (ETD) creates serious privacy concerns. For instance, these detailed readings can reveal consumers' habits, such as whether they are at home or away, the number of people in the household, and the appliances they are using [9]. This information could be exploited to target homes when occupants are absent or sold to insurance companies to adjust plans based on consumer behavior. According to the Electronic Privacy Information Center, the revelation of personal behavior pattern is a significant privacy concern in the SG, and thus power consumption data should be protected from unauthorized access [10].

Several advanced methods have been proposed to detect electricity theft while protecting consumer privacy. Yao et al. [11] used Paillier encryption to secure data during collection, ensuring privacy but suffering from low accuracy and heavy computational demands. Similarly, Nabil et al. [8] developed a scheme using secret sharing and secure computation with a CNN model, which secures data but has high computation and communication costs, limiting its use in practice. Ibrahem et al. [12] addressed these issues with functional encryption, simplifying theft detection without interactive sessions, though at the cost of detection accuracy. These methods rely on Feed Forward Neural Network (FFN)

and 1-D CNN models, which fail to adequately capture the temporal correlations and periodicity inherent in electricity consumption data. As noted in previous studies [11], [13], [14], leveraging consumers' daily and weekly consumption patterns using LSTM and CNN, effectively extracting rich features, and capturing temporal dynamics.

To address the limitations to existing techniques, we propose an efficient and privacy-preserving ConvLSTM-based detection of electricity theft cyber-attacks. The summary of our contribution and novelty are described as follows:

- We developed a novel Conv-LSTM detector that integrates a 2-D CNN model with an LSTM network. This combination enhances the detection capability by automatically extracting high-level periodic features and the day-to-day power consumption data correlation from the consumers' electricity consumption patterns, organized in a 2-D matrix format based on hours and days. This approach significantly improves the model's functionality and detection accuracy, specifically addressing the inherent periodicity and temporal dependencies in electricity consumption data.
- We have developed a general-purpose and lightweight IPFE scheme based on secure inner product using linear invertible matrices. To the best of our knowledge, there exists, no such a secure and lightweight IPFE scheme in the literature.
- We have integrated our proposed IPFE scheme with the proposed ETD model to allow consumers to send their encrypted power consumption data to the EU, which then computes the resulting feature map of the first convolutional layer of the ETD model without accessing the raw power consumption readings, thus protecting consumer privacy.

The remainder of this article is organized as follows. section II presents the related works. The considered system model, threat model, and design objectives are discussed in section III. Preliminaries and background are presented in section IV. In section V we give the details of the proposed scheme and the detection model architecture. Discussions, evaluations, and experiments are presented in section VI. Finally, our conclusions are drawn in section VII.

II. RELATED WORKS

A. NON-PRIVACY-PRESERVING DETECTION

Various methods have been utilized in the literature to detect electricity theft attacks in the SG, including hardware-based approaches [18], game theory [19], matrix decomposition [20], linear regression [21], state estimation [22] and machine learning based methods [8], [11], [12], [13], [16], [23], [24], [25], [26], [27], [28]. Hardware-based solutions, involving additional equipment like wireless sensors, distribution transformers, and smart meters incur a high implementation cost. The game theory-based approach formulates the electricity theft detection problem as a game between the electric utility and fraudulent consumers, where the difference in electricity consumption behavior determines the game's outcome. However, defining utility functions for all players using statistical anomaly detection proves challenging. In other methods like matrix decomposition [20], linear regression [21], and state estimation methods [22], there are limitations related to handling large datasets and vulnerability to false data injection [29]. The study in [30] demonstrated how smart meters can be leveraged for voltage monitoring and control, addressing last-mile voltage stability issues in smart grids. This highlights the growing importance of smart meters in grid management and stability. Furthermore, the study [31] proposed a comprehensive smart meter infrastructure for IoT applications in smart grids, showcasing the potential of these devices to enable advanced functionalities and improve overall grid performance. In the context of energy theft, the authors in [32] provided an in-depth analysis of smart metering in the European Union and its relation to the energy theft problem. Their work underscores the significance of addressing energy theft in modern smart grid systems and the role of advanced metering infrastructure in detection and prevention strategies.

ML methods are currently adopted for electricity theft classification in the smart grid. These include traditional ML-based approaches, such as support vector machines [24], decision tree [26], linear regression [21] and gradient boosting [27]. Additionally, Deep Learning (DL)-based approaches, such as Recurrent Neural Network (RNN) [28], [33], [34] and CNN [8], [11], [13], [14] are utilized. A hybrid detector using a CNN-LSTM approach for electricity theft detection is proposed in [35]. Our work is different in the following aspects: first, [35] requires access to private power consumption data, raising privacy concerns, whereas our model operates on encrypted data, protecting consumer privacy. Second, our model can utilize the day-to-day power consumption correlation matrix as an input, enhancing the ability to detect fraudulent use. Last, we employ the ADASYN technique for synthetic data generation to address class imbalance. Unlike SMOTE used in [35], ADASYN accounts for the density of minority class examples, reducing overfitting and improving generalization.

To sum up, despite the effectiveness of ML/DL approaches, they inherently reveal sensitive information to unauthorized individuals and trusted entities. This practice is sufficient to build up many details of the user's daily life such as electric appliance usage, time householders leave or return home, and the number of occupants in a house. This poses a threat to user privacy. Therefore, integrating machine learning approaches with data privacy preservation is essential to prevent the exposure of sensitive data to entities within the grid.

B. PRIVACY-PRESERVING DETECTION

Privacy preservation scheme developed in [8], [12], and [11] utilize DL methods for detecting electricity thefts while preserving consumers' privacy. In the scheme proposed by Yao et al. [11], Paillier encryption is employed to protect user privacy during data collection. However, their scheme suffers

TABLE 1. Comparison of related works in the literature.

Schemes	Proposed Scheme	Yao et al [11]	Ibrahem et al [12]	Nabil et al [8]	Xia et al [15]	Gao et al [16]
Dataset	IRISH [17]	SGCC [14]	IRISH	IRISH	-	SGCC
Deep learning Technique	2-D CNN-LSTM	2-D CNN	FNN	1-D CNN	1-D CNN	CONVLSTM2D
Privacy	SIP	HE	IPFE	SPDZ Protocol	FHE	No privacy
2-D Extraction	✓	✓	×	×	×	✓
Deeper and Long-term Features Extraction	✓	×	×	×	×	✓
Data Balancing Technique	ADASYN	Not handled	ADASYN	ADASYN	-	borderline-SMOTE

SIP: Secure Inner Product IPFE: Inner Product Functional Encryption HE: Homomorphic Encryption FHE: Fully Homomorphic Encryption
ADASYN: Adaptive Synthetic Sampling SMOTE: Synthetic Minority Oversampling Technique

from low accuracy and high computation overheads imposed by the aggregating entity. Nabil et al. [8] developed a privacy preservation scheme for theft detection using deep learning methods Their approach uses secret sharing techniques to mask the fine-grained power consumption reported by the SMs. The EU uses aggregated masked readings for theft detection without learning the individual consumption readings. This is achieved through a secure multiparty computation protocol evaluated on a CNN model using arithmetic and binary circuits. The CNN model's evaluation is done through an interactive/online session between the individual smart meters and the EU. However, their scheme has the following drawbacks. The proposed scheme requires high computation and communication overhead because the SMs and EU should execute the CNN model in an online interactive way to detect theft while preserving consumer privacy. Also, it takes a total time of 48 min and exchanged data of 1900 MB for a single SM to be evaluated. Further, another overhead occurs for using the secret sharing technique to mask the consumption readings. The large computation and communication overheads are impractical to cost-effective devices with limited computation capability and low bandwidth communications.

Ibrahem et al. [12] addressed these limitations in [8] by offering a privacy-preserving power theft detection using functional encryption. This approach encrypts each user's smart meter readings using secret keys from a trusted authority and then decrypts the encrypted readings with the help of a decryption key from the same entity. The smart meters do not require an interactive session to evaluate the power theft detector. Also, the result of detection result is only known to the EU and no entity is allowed to learn the readings of other consumers; hence the privacy of consumers is being preserved. In addition, the scheme demonstrates satisfactory communication and computation overheads. However, the detection model exhibits low accuracy in electricity theft classification.

The methods proposed in [8] and [12] utilize FFN and 1-D CNN detection models, respectively, as they have shown to be a better choice than other feature extraction in previous publications. However, both FNN and 1-D CNN models have limitations. One key limitation lies in their inability

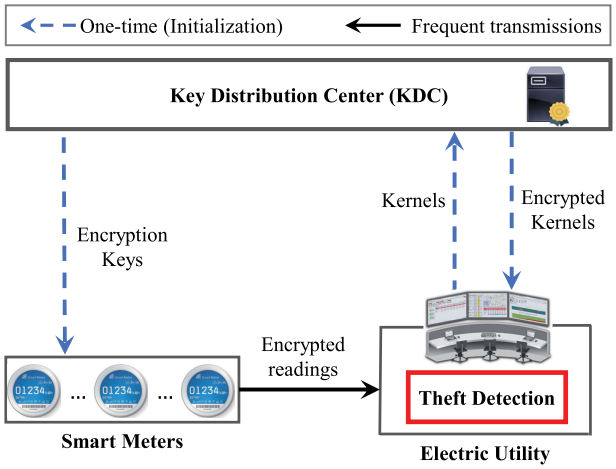

FIGURE 2. System model.

to model the temporal correlation and periodicity inherent in the time series nature of electricity consumption, which affects their ability to capture the periodicity characteristic of users' electricity consumption patterns. This adversely impacts the models' functionality and detection accuracy. To address this limitation, we introduce a novel approach using a 2-D CNN-LSTM architecture for electricity theft detection. The 2-D CNN automatically extracts high-level features from users' daily electricity consumption data arranged in a 2-D matrix based on hours and days while the LSTM network is designed to capture temporal and long-term dependencies. Extensive research has demonstrated the superior performance of 2-D CNN models for electricity theft detection, as demonstrated in studies like [11], [13], and [14]. Their performance evaluations indicate that 2-D CNN outperforms 1-D CNN models in detecting energy theft. As a summary, Table 1 provides a comprehensive comparison of various methods utilized in the literature for detecting electricity theft. It categorizes each method based on its core approach, data balancing, and performance, and evaluates whether it includes privacy preservation measures.

III. SYSTEM MODEL

This section discusses the considered network and threat models, along with the design goals of the proposed scheme.

A. NETWORK MODEL

Our network model, as depicted in Figure 2, consists of three core entities within the smart grid configuration: the electric utility (EU), a set of smart meters (SMs) installed at the consumers' premises, and a Key Distribution Center (KDC). The role of each entity is described as follows:

- **Key Distribution Center**: The KDC is responsible for generating and distributing a unique encryption key for each SM. Also, the KDC receives a set of kernels from the EU and uses them to generate a set of functional decryption kernels that are sent back to the EU. Key generation and distribution is a one-time process that runs only during the system's initialization phase. After that, the KDC does not actively participate in the electricity theft detection process.
- **Smart meters**: SMs are key components of the AMI network, designed specifically to measure and report the flow of electricity from the power grid to consumer premises. We consider a set of smart meters $\mathbb{SM} = \{\text{SM}_i, 1 \leq i \leq |\mathbb{SM}|\}$ where each consumer house is equipped with a SM that reports encrypted power consumption data to the EU for data analysis, billing purposes, and electricity theft detection.
- **Electric Utility**: The EU is responsible for processing and analyzing data reported by SMs. The EU utilizes the reported encrypted power consumption readings sent by each SM and passes them to the proposed electricity theft detection model. The EU relies on the outcomes of the theft detection system to make informed decisions regarding grid operations, ensuring grid stability, and preventing potential disruptions.

B. THREAT MODEL AND DESIGN GOALS

The EU is considered an honest-but-curious entity, meaning it adheres to the proposed protocol correctly but might attempt to learn the individual power consumption patterns of consumers from the encrypted power consumption data reported by the smart meters. The customers' power consumption readings could reconstruct sensitive information about consumer lifestyles, including details such as when customers are at home or away, the types and quantities of smart appliances in use, and the number of occupants in a household. On the other hand, consumers may act maliciously in two ways. First, a malicious consumer may tamper with their SM and report false consumption readings to the EU to illegally reduce their bills for financial gain. Such malicious activity not only leads to financial losses for the EU but also may impact the decisions taken by the EU to manage the grid. Second, a consumer may try to use their keys to learn the power consumption data of other consumers. Furthermore, there exists a malicious external adversary who eavesdrops on the communication between the smart meters and the utility aiming to learn sensitive information about consumers.

Based on the problem definition and the aforementioned threat model, the design goals of our proposed scheme are as follows.

- **Privacy Preservation**: The proposed scheme shall ensure that individual consumer power consumption data remains confidential and cannot be inferred by either the EU in its honest-but-curious role or by external adversaries through eavesdropping. This goal aims to protect sensitive information about consumers' lifestyles and habits derived from their power usage patterns.
- **Electricity Theft Detection**: The proposed scheme shall enable the EU to execute an electricity theft detection model using the encrypted power consumption readings to identify malicious consumers.
- **Efficiency**: The proposed scheme should be efficient in terms of computation overhead. This ensures that the system remains practical for use in real-time applications and does not introduce significant delays or costs in the processing and transmission of power consumption data.

IV. PRELIMINARIES

A. FUNCTIONAL ENCRYPTION

Functional Encryption (FE) is an encryption paradigm enabling an encryptor to encrypt a message m using a key k, resulting in $Enc_k(m)$. This setup allows a decryptor possessing a decryption key dk to learn only a specific function's output computed on the message, rather than the full plaintext m. Formally, this is represented as $Dec_{dk}(Enc_k(m)) = f(m)$ [36]. Recently, there has been a growing emphasis on how to design efficient FE schemes for limited classes of functions or polynomials, such as linear [37], [38] or quadratic [39].

This work introduces a novel approach to inner product functional encryption (IPFE), a subtype of FE that facilitates calculating the inner product of two encrypted vectors. Within the IPFE model, encryption of a vector $\mathbf{r}$ using key k, allows a decryptor, who has functional decryption key $dk_{\mathbf{w}}$ derived from another vector $\mathbf{w}$ and k, to exclusively compute the dot product $(\mathbf{r} \cdot \mathbf{w})$ upon decrypting $\mathbf{r}$'s encrypted representation, without access to $\mathbf{r}$'s individual components. The IPFE framework encompasses three primary algorithms described below:

- *Key Generation*: This algorithm is executed by KDC and it involves generating an encryption key k and dispatching it to the encryptor. Concurrently, the KDC acquires a vector $\mathbf{w}$ from the decryptor, utilizes $\mathbf{w}$ and k to generate a functional decryption key $dk_{\mathbf{w}}$, and sends it back to the decryptor.
- *Encryption*: This algorithm is executed by an encryptor who employs the secret key k to encrypt the plaintext vector $\mathbf{r}$ and forwards the resultant ciphertext vector $\mathbf{ct}$ to the decryptor.
- *Decryption*: This algorithm is executed by the decryptor, who uses the received ciphertext $\mathbf{ct}$ and the functional

decryption key $dk_{\mathbf{w}}$ obtained from the KDC to compute and retrieve $(\mathbf{r} \cdot \mathbf{w})$, without gaining access to the individual components of $\mathbf{r}$. The decryptor is obliged to maintain non-collusion with the KDC.

B. SECURE INNER PRODUCT

Secure inner product (SIP) over encrypted data have found widespread application in various domains like secure keyword searching [40], [41], secure data collection and aggregation for smart grid AMI networks [42], [43], and privacy-preserving location-based applications [44], [44], [45]. In this technique, data are represented in the form of vectors where the main idea of the SIP technique is to enable secure dot product computations between two data vectors without revealing the content of the two vectors. In specific, the vectors are encrypted using linear invertible matrices such that when a dot product operation is computed between two encrypted vectors, it would result in the dot product result of the plaintext data vectors. In this paper, we developed a novel IPFE scheme that utilizes the SIP algorithms allowing the EU to generate the resulting feature map of the first convolutional layer of a 2D Convolutional Neural Network (CNN) model. This means the EU can compute the convolution result using encrypted data without accessing the raw data.

C. CONVOLUTIONAL NEURAL NETWORK

CNN finds widespread use in domains such as speech processing, image processing [25], models like VGG and ResNet [11], and natural language processing (NLP) [16]. There exists a variant of CNNs, called 2-D CNN, for processing 2-D matrices of data. The typical architecture of 2-D CNN consists of an input layer, an output layer, and multiple hidden layers, where the hidden layers consist of three main parts: the convolutional layer, the pooling layer, and the fully connected layer. The convolutional layer consists of a group of parallel, learnable filters or kernels to extract different features from the input data by convolving the sliding window containing the filter's weight with the input data. During the forward pass, each filter traverses the input data with a certain stride, allowing the filter's weights to engage in convolution operation with the input data to produce a 2-D activation map. The size of the feature map generated depends on the input data size and kernel size. The 2-D activation map is a group of feature maps corresponding to the group of filters. It is regarded as a collection of feature maps, each of which corresponds to one of the filters in the group. The feature maps are fed into the pooling layer responsible for reducing the dimensionality (spatial size) of the input. This dimensional reduction is achieved through nonlinear down sampling to progressively decrease the number of parameters, controlling overfitting and computation complexity. After several convolution and max pooling layers, the high-level reasoning in the network is done via a fully connected layer. The fully connected layer is used to generate the final output and neurons within the fully connected layer have connections to all activations in the previous layer. The final output from CNN is encapsulated into time-distributed layers [46] which helps in maintaining the temporal information and enables the network to learn from the sequential nature of the data. The extracted features from the time-distributed layers are flattened for use in the LSTM network. Importantly, in this work, LSTM is chosen over pooling layers in CNN to reduce the loss of detailed local information and capture long-term dependencies in sequences [16].

D. LONG AND SHORT TERM MEMORY

LSTM network, a type of recurrent neural network (RNN), is trained using time backpropagation [28]. Its architecture is fundamentally different from traditional feedforward neural networks and proves more efficient than other RNNs due to its unique design that effectively addresses the challenges that hinder the training and scalability of other RNN variants. The key innovation of LSTMs lies in their architecture, which is specifically designed to avoid the vanishing and exploding gradient problems that often plague RNNs during training. LSTMs are adept at processing sequential data, making them ideal for applications such as language translation, speech recognition, and time-series analysis. This capability stems from their ability to maintain a form of memory that incorporates previous information into the current context, thereby understanding the temporal dynamics of data. At the heart of the LSTM's architecture is the memory cell, designed to store information over extended periods. This memory cell is regulated by three gates: the forget gate f_t, which filters out irrelevant historical data by deciding which parts of the previous cell state, $C_{(t-1)}$ to retain and which are discarded; the input gate I_t, which controls the addition of new information to the cell state; and the output gate, which decides the information from the cell state to be used in computing the output. The output of the LSTM cell at a time t, denoted as h_t, is dependent not only on the current input x_t but also on the previous output $h_{(t-1)}$. In addition, the outputs from the forget and the input gates are combined to update the cell state, C_t. Finally, the output gate determines the parts of the cell state to be propagated to the next LSTM cells. These gates enable the LSTM to selectively update its memory by learning what information is relevant to retain or discard, thus capturing long-term dependencies without falling prey to gradient-related issues.

Training LSTMs involves the use of Truncated Back-propagation Through Time (TBPTT) [33], a modification of the standard backpropagation technique suited for temporal sequences. TBPTT limits the number of time steps over which gradients are backpropagated, thereby simplifying the computational process and mitigating the vanishing gradient problem. In applications such as predicting the long-term consumption patterns of residents, LSTMs can abstract and retain essential information over long durations.

The classical LSTM equations [28] can be represented as follows: the input gate Equation (1), the forget gate

Equations (2), and the output gate Equation (4). In addition, Equation (3) denotes the cell output of the LSTM node at time step t. Equation (5) shows the hidden state of the LSTM node at time step t.

$$I_t = \sigma(W_{x_I} x_t + W_{h_I} h_{t-1} + b_I) \quad (1)$$

$$f_t = \sigma(W_{x_f} x_t + W_{h_f} h_{t-1} + b_f) \quad (2)$$

$$C_t = f_t \circ C_{t-1} + I_t \circ tanh(W_{x_c} x_t + W_{h_c} h_{t-1} + b_c) \quad (3)$$

$$O_t = \sigma(W_{x_o} x_t + W_{h_o} h_{t-1} + b_o) \quad (4)$$

$$h_t = O_t \circ tanh(C_t) \quad (5)$$

where σ denotes the sigmoid function, $\circ$ denotes the Hadamard product, and b is the bias vector parameter. $W_{x_I}, W_{x_f}, W_{x_c}, W_{x_o}$ are weighted for the input x_t of the input gate, forget gate, cell state, and output gate, respectively. $W_{h_I}, W_{h_f}, W_{h_c}, W_{h_o}$ are weights for the previous output h_{t-1}. Parameters $W_{x_I}, W_{x_f}, W_{x_c}, W_{c_o}, W_{h_I}, W_{h_f}, W_{h_c}, W_{h_o}$ are learned during the training phase to control the memory and forget of the LSTM.

TABLE 2. Main notations.

Notation	Description
$\mathbb{SM}$	Set of smart meters $\mathbb{SM} = \{SM_i, 1 \leq i \leq \lvert\mathbb{SM}\rvert\}$
$\mathcal{MK}$	The KDC's Master key set
$\mathbf{sv}$	Binary splitting vector
SM_i	i-th smart meter
$\mathcal{EK}_i$	Encryption key set of SM_i
$\mathbf{R}_i$	2D power consumption data of SM_i
$\mathbf{r}_i$	Flattened version of $\mathbf{R}_i$
q	Length of the flattened vector $\mathbf{r}_i$
$\mathbf{ct}_i$	Ciphertext vector computed by SM_i for $\mathbf{r}_i$
$\mathbf{W}$	2D CNN Kernel
$\mathbf{F}$	Feature map resulting from $\mathbf{R} * \mathbf{W}$
f_{jk}	a feature value in $\mathbf{F}$ at row j and column k
$\mathbf{W}_{ij}$	Expanded kernel to compute f_{jk}
$\mathbf{w}_{jk}$	Flattened version of $\mathbf{W}_{jk}$
$\mathbf{dk}_{\mathbf{w}_{jk}}$	Functional decryption key associated with vector $\mathbf{w}_{jk}$

V. PROPOSED SCHEME

In this section, we give the details of our proposed scheme. For ease of readability, we list in Table 2 the main notations used in this section. Moreover, to differentiate between vectors and matrices, we use lowercase bold notation for vectors and uppercase bold notation for matrices. For example, $\mathbf{r}$ represents a vector whereas $\mathbf{M}$ represents a matrix.

A. OVERVIEW

Figure 3 shows an overview of the proposed scheme. During the system initialization, the KDC generates a master secret key $\mathcal{MK}$ that is used to derive a unique encryption key $\mathcal{EK}_i$ for each smart meter SM_i. In addition, the EU sends the set of the kernels of the first convolutional layer in our electricity theft detection model to the KDC which uses them with the master key $\mathcal{MK}$ to generate the set of functional decryption keys where a functional decryption key $\mathbf{dk}_{\mathbf{w}_{jk}}$ represents the functional decryption key of a kernel $\mathbf{W}_{jk}$. The KDC send the functional decryption keys back to the EU. After the system initialization, the KDC is no longer involved in the regular and repeated operation of electricity theft detection. Further details about the system initialization will be provided in subsubsection V-B.

In order to run the electricity theft model over encrypted readings to ensure the confidentiality of the consumer's power consumption data, we developed a novel IPFE technique based on the secure element-wise product technique proposed in our earlier work [47] as follows. First, SM_i encrypts the power consumption data of the reporting period $\mathbf{R}_i$ using its encryption key $\mathcal{EK}_i$ as will be explained in subsubsection V-C and sends the generated ciphertext $\mathbf{ct}_i$ to the EU. Then, EU will run the secure convolution computation using the received ciphertexts and the set of the functional decryption keys as will be explained in subsubsection V-D to securely compute the resulting feature map of the first convolutional layer without accessing the individual power consumption readings to preserve the consumer's privacy. Finally, the output of the secure convolution computation will be passed to the rest of the detection model as shown in subsubsection V-E to conclude the detection results.

B. SYSTEM INITIALIZATION

System initialization is carried out by the KDC and is comprised of three phases: (1) generation of the master key; (2) generation of the SMs' encryption keys; and (3) generation of the EU's functional decryption keys.

1) GENERATION OF THE MASTER KEY

The KDC generates a random binary vector $\mathbf{sv}$ of size q to be used as a splitting indicator for the SIP technique. The KDC also generates a master key set $\mathcal{MK} = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3, \mathbf{N}_4\}$ where each element in $\mathcal{MK}$ is a square invertible random matrix of order q. $\mathcal{MK}$ is used to derive both the encryption and functional decryption keys for all the smart meters and EU respectively.

2) GENERATION OF SM'S ENCRYPTION KEYS

The KDC use $\mathcal{MK}$ to derive a unique encryption key denoted by $\mathcal{EK}_i$ for each SM_i. $\mathcal{EK}_i$ consists of 4 components as shown in Equation (6) where $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i, \mathbf{D}_i$, are square invertible random matrices of order q such that $\mathbf{A}_i + \mathbf{B}_i = \mathbf{M}_1$ and $\mathbf{C}_i + \mathbf{D}_i = \mathbf{M}_2$. Finally, the KDC sends $\mathcal{EK}_i$ to smart meter SM_i.

$$\mathcal{EK}_i = \left[\mathbf{A}_i\mathbf{N}_1 \;\; \mathbf{B}_i\mathbf{N}_2 \;\; \mathbf{C}_i\mathbf{N}_3 \;\; \mathbf{D}_i\mathbf{N}_4\right] \quad (6)$$

3) GENERATION OF EU'S FUNCTIONAL DECRYPTION KEYS

As mentioned earlier, the EU sends the set of the kernels of the first convolutional layer in the electricity theft detection model to the KDC. Then, the KDC generates the set of expanded kernels. To generate a functional decryption key associated with an expanded kernel $\mathbf{W}_{jk}$, the KDC first

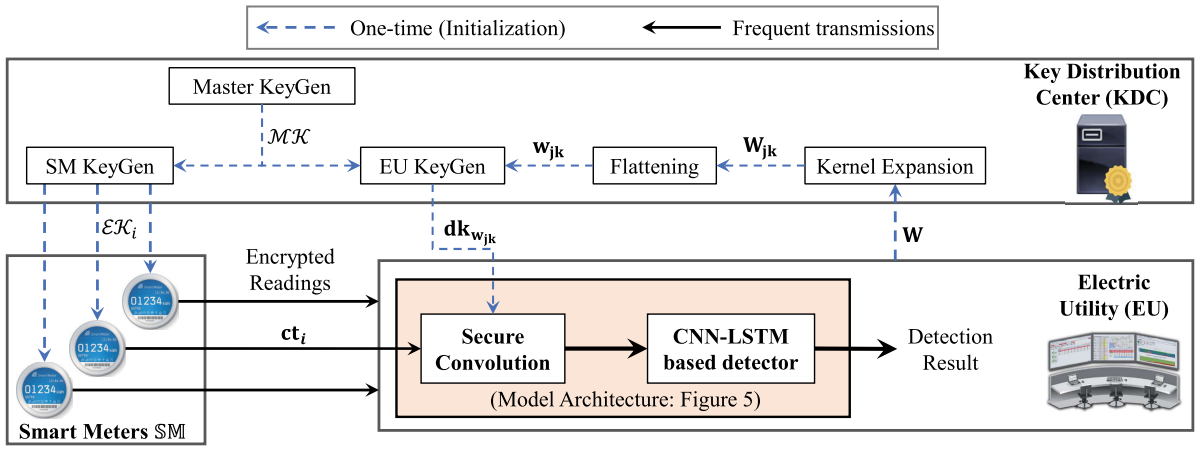

FIGURE 3. Illustration of the proposed scheme.

flattens the expanded kernel $\mathbf{W}_{jk}$ to $\mathbf{w}_{jk}$, i.e., reshaping the matrix $\mathbf{W}_{jk}$ into a vector $\mathbf{w}_{jk}$. This is a necessary step as the SIP technique works for vectors not for matrices.

The KDC uses the binary vector $\mathbf{sv}$ to split the vector $\mathbf{w}_{jk}$ into two random column vectors $\mathbf{w}'_{jk}$ and $\mathbf{w}''_{jk}$ of same size. The splitting method is described as follows. If the z^{th} bit of $\mathbf{sv}$ equals 1, then both $\mathbf{w}'_{jk}(z)$ and $\mathbf{w}''_{jk}(z)$ are set similar to $\mathbf{w}_{jk}(z)$, while if z^{th} bit of $\mathbf{sv}$ equals 0, then, $\mathbf{w}'_{jk}(z)$ and $\mathbf{w}''_{jk}(z)$ are set to two random numbers such that their sum is equal to $\mathbf{w}_{jk}(z)$. Following the splitting operation, the KDC generates the functional decryption key $\mathbf{dk}_{\mathbf{w}_{jk}}$ using $\mathbf{w}'_{jk}$, $\mathbf{w}''_{jk}$ and $\mathcal{MK}$ as

$$\mathbf{dk}_{\mathbf{w}_{jk}} = \begin{bmatrix} \mathbf{N}_1^{-1}\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\ \mathbf{N}_2^{-1}\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\ \mathbf{N}_3^{-1}\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \\ \mathbf{N}_4^{-1}\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \end{bmatrix} \tag{7}$$

Finally, the KDC sends all the functional decryption keys back to the EU.

C. REPORTING POWER CONSUMPTION READINGS

During the reporting period, each SM_i uses $\mathcal{EK}_i$ to encrypt its power consumption data $\mathbf{R}_i$. First, $\mathbf{R}_i$ is flattened into a vector $\mathbf{r}_i$. Then, SM_i uses the splitting vector $\mathbf{sv}$ to split the vector $\mathbf{r}_i$ into two random row vectors $\mathbf{r}'_i$ and $\mathbf{r}''_i i$. The splitting method is the opposite of what was done to split $\mathbf{w}_{jk}$, i.e., if the z^{th} bit of $\mathbf{sv}$ equals 0, then both $\mathbf{r}'_i(z)$ and $\mathbf{r}''_i(z)$ are set similar to $\mathbf{r}_i(z)$, while if z^{th} bit of $\mathbf{sv}$ equals 1, then, $\mathbf{r}'_i(z)$ and $\mathbf{w}''_i(z)$ are set to two random numbers such that their sum is equal to $\mathbf{r}_i(z)$. Finally, SM_i uses his encryption key $\mathcal{EK}_i$ to generate the ciphertext $\mathbf{ct}_i$ as

$$\mathbf{ct}_i = \left\{\mathbf{r}'_i\mathbf{A}_i\mathbf{N}_1 \;\; \mathbf{r}'_i\mathbf{B}_i\mathbf{N}_2 \;\; \mathbf{r}''_i\mathbf{C}_i\mathbf{N}_3 \;\; \mathbf{r}''_i\mathbf{D}_i\mathbf{N}_4\right\} \tag{8}$$

After generating $\mathbf{ct}_i$, SM_i sends it to the EU to be used for the electricity theft detection evaluation.

D. CONVOLUTION COMPUTATION OVER ENCRYPTED READINGS

Figure 4 visualizes how the convolution operation can be computed via a series of Hadamard products or element-wise products denoted by $\odot$. In order to compute $\mathbf{F} = \mathbf{R} * \mathbf{W}$, the convolution kernel $\mathbf{W}$ should slide along the input data $\mathbf{R}$ to generate a feature map $\mathbf{F}$. This can be done as follows. As shown in the figure, the first step is to use $\mathbf{W}$ to generate a set of expanded kernels where each expanded kernel has the same dimensions as $\mathbf{R}$. These expanded kernels represent all the possible positions of sliding of $\mathbf{W}$ over $\mathbf{R}$. Then, the element-wise product between $\mathbf{R}$ and each expanded kernel would result in the corresponding element in $\mathbf{F}$. For example, $f_{11} = \mathbf{R} \odot \mathbf{W}_{11}$. Note that, padding the data matrix $\mathbf{R}$ before the convolution process only affects the size of the expanded kernel, and computing convolution over padded data is still possible using the element-wise product technique.

Using the aforementioned idea, the EU can securely build the feature map of the first convolutional layer of the detection model by utilizing both the received ciphertext $\mathbf{ct}_i$ and the set of functional decryption keys. Note that, the functional decryption key $\mathbf{dk}_{\mathbf{w}_{jk}}$ was designed such that when multiplied by $\mathbf{ct}_i$ it would result in the dot product of the flattened vectors $\mathbf{r}_i$ and $\mathbf{w}_{jk}$ which is equivalent to Hadamard product of the plaintext power consumption data $\mathbf{R}_i$ and expanded kernel $\mathbf{W}_{jk}$ as illustrated above. The proof of correctness of computing the feature f_{jk} from the ciphertext $\mathbf{ct}_i$ is

$$\begin{aligned} f_{jk} = \mathbf{ct}_i \cdot \mathbf{dk}_{\mathbf{w}_{jk}} &= \mathbf{r}'_i\mathbf{A}_i\mathbf{N}_1\mathbf{N}_1^{-1}\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\ &+ \mathbf{r}'_i\mathbf{B}_i\mathbf{N}_2\mathbf{N}_2^{-1}\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\ &+ \mathbf{r}''_i\mathbf{C}_i\mathbf{N}_3\mathbf{N}_3^{-1}\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \\ &+ \mathbf{r}''_i\mathbf{D}_i\mathbf{N}_4\mathbf{N}_4^{-1}\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \\ &= \mathbf{r}'_i\mathbf{A}_i\mathbf{M}_1^{-1}\mathbf{w}'_{jk} + \mathbf{r}'_i\mathbf{B}_i\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\ &+ \mathbf{r}''_i\mathbf{C}_i\mathbf{M}_2^{-1}\mathbf{w}''_{jk} + \mathbf{r}''_i\mathbf{D}_i\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \end{aligned}$$

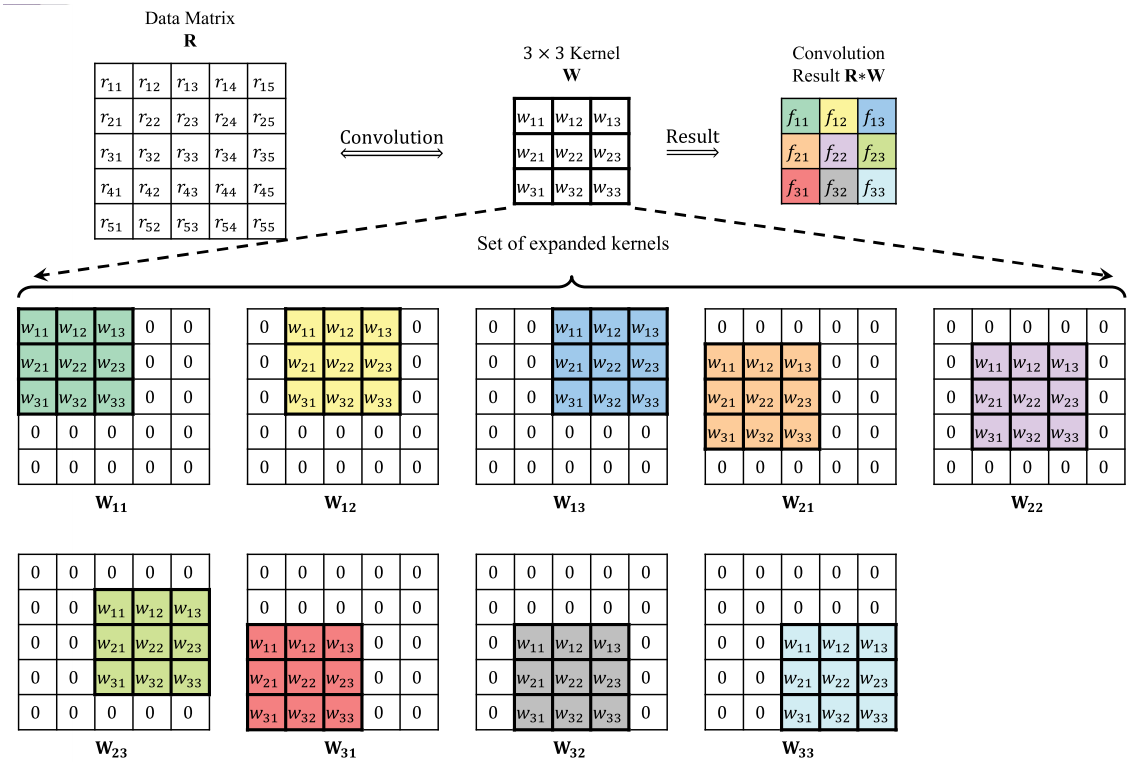

FIGURE 4. Visualizing convolution as an element-wise product between the data matrix **R** and the set of expanded kernels $\mathbf{W_{jk}}$.

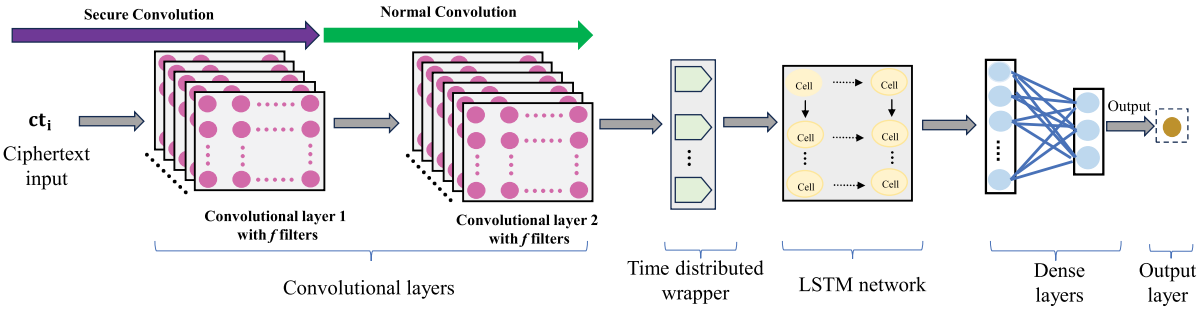

FIGURE 5. The proposed 2-D CNN LSTM architecture.

$$
\begin{aligned}
&= \mathbf{r}'_i(\mathbf{A}_i + \mathbf{B}_i)\mathbf{M}_1^{-1}\mathbf{w}'_{jk} \\
&\quad + \mathbf{r}''_i(\mathbf{C}_i + \mathbf{D}_i)\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \\
&= \mathbf{r}'_i\mathbf{M}_1\mathbf{M}_1^{-1}\mathbf{w}'_{jk} + \mathbf{r}''_i\mathbf{M}_2\mathbf{M}_2^{-1}\mathbf{w}''_{jk} \\
&= \mathbf{r}'_i\mathbf{w}'_{jk} + \mathbf{r}''_i\mathbf{w}''_{jk} \\
&= \mathbf{r}_i \cdot \mathbf{w}_{jk} = \mathbf{R}_i \odot \mathbf{W}_{jk}
\end{aligned}
$$

In this way, the EU can build the entire feature maps and pass them to the subsequent layers of the detection model.

E. ELECTRICITY THEFT DETECTION

In our proposed architecture for electricity theft detection, as depicted in Figure 5, we employ a sequence of layers designed to analyze electricity consumption data for the identification of theft patterns. This architecture is constructed to leverage the strengths of both spatial and temporal data analysis through the integration of CNNs and LSTM networks, further refined by dense layers leading to the final output layer. The initial processing of the electricity consumption data is performed by secure and normal convolutional layers. These layers apply a series of filters to the input data to extract significant spatial features. The transformation at this stage can be represented as:

$$\mathbf{F}_2 = \sigma(\mathbf{W}_c * \mathbf{F}_1 + \mathbf{B}_c) \tag{9}$$

where $\mathbf{F}_2$ represents the feature maps produced by the convolutional layers, $\mathbf{W}_c$ denotes the weights of the convolutional filters, $\mathbf{F}_1$ is the input data matrix, $\mathbf{B}_c$ is the bias, $*$ denotes the convolution operation, and σ is the activation function. After spatial features are extracted by the convolutional layers, a time-distributed wrapper is applied. This wrapper allows the model to process each time step of the input data separately but in parallel, preparing the data for sequential analysis by the LSTM network. This process can be described as:

$$\mathbf{F}_{td} = \tau(\mathbf{F}_2) \tag{10}$$

where $\mathbf{F}_{td}$ represents the time-distributed features and τ symbolizes the time-distribution operation over the convolutional feature maps $\mathbf{F}_2$. The LSTM network receives the time-distributed features and performs temporal analysis to capture long-term dependencies within the data. The transformation by the LSTM layer can be encapsulated as:

$$\mathbf{F}_{lstm} = \text{LSTM}(\mathbf{F}_{td}) \tag{11}$$

where $\mathbf{F}_{lstm}$ denotes the output feature vector from the LSTM layer, capturing both spatial and temporal dynamics of the electricity consumption data. Following the LSTM network, one or more dense layers are employed to further process the features. These layers perform high-level reasoning based on the extracted features:

$$O = \phi(\mathbf{W}_d \cdot \mathbf{F}_{lstm} + \mathbf{b}_d) \tag{12}$$

where O represents the final output indicating the detection of electricity theft, $\mathbf{W}_d$ are the weights, $\mathbf{b}_d$ is the bias, and ϕ is the activation function of the dense layers.

VI. DISCUSSIONS AND EXPERIMENT

A. CONSUMERS' PRIVACY PRESERVATION

As shown in subsubsection V-C, the power consumption data represented in $\mathbf{r}_i$ is split into two vectors $\mathbf{r}'_i$ and $\mathbf{r}''_i$ that is encrypted using the unique encryption key $\mathcal{EK}_i$ to generate $\mathbf{ct}_i$. The security of this encryption algorithm has been proven in the known ciphertext model [48]. Thus, $\mathbf{r}'_i$ and $\mathbf{r}''_i$ cannot be extracted from $\mathbf{ct}_i$ and hence $\mathbf{r}_i$ is protected against the EU or external adversaries. Moreover, each user receives a unique secret encryption key from the KDC generated from the master key set $\mathcal{MK}$. Therefore, a smart meter SM_j who has an encryption key $\mathcal{EK}_j$ cannot decrypt the ciphertext generated by another smart meter SM_i [49]. Finally, as shown in subsubsection V-D, the proposed IPFE scheme allows the EU to use the decryption key $\mathbf{dk}_{\mathbf{w}_{jk}}$ to only extract $\mathbf{r}_i \cdot \mathbf{w}_{jk}$ but not $\mathbf{r}_i$. Therefore, the proposed scheme ensures the confidentiality of the individual power consumption data against other consumers, the EU, and external adversaries and hence preserves the consumers' privacy.

B. EXPERIMENT SETUP

1) HARDWARE CONFIGURATION

The experiments were using an conducted on Intel(R) Core(TM) i7-10700 CPU at 2.90GHz with 16.0 GB of RAM. This configuration ensured adequate computational power to handle the requirements of our cryptographic methods and deep learning algorithms.

2) DATASET

We utilized a dataset from the Irish Smart Metering Trials, which was compiled by Electric Ireland and the Sustainable Energy Authority of Ireland (SEAI) in January 2012 [17]. This dataset includes electricity consumption data for more than 4,000 smart meters over 536 days, spanning the years 2009 to 2010. Each smart meter in the dataset recorded a total of 25,728 readings. For this study, we focused on a subset of 2,000 smart meters ($|\mathbb{SM}| = 2000$), with each meter providing 48 readings per day.

3) ELECTRICITY THEFT ATTACKS

In the dataset, all consumption readings originate from honest consumers, which poses a challenge for having fraudulent readings from malicious smart meters. To address this, we created a synthetic dataset to simulate conditions of electricity theft, employing the methodologies outlined in [24]. Table 3 presents a detailed overview of the simulated attacks, which include three primary types: partial reduction, bypass filters, and price-based load control. We denote the j^{th} electricity reading from SM_i on day d as $\mathbf{r}_i[t]$. Each attack function $f(\cdot)$ was specifically designed to modify the reported energy consumption $\mathbf{r}_i[t]$ to emulate various scenarios of electricity theft. Each attack below is applied over specific time frames defined as intervals. For instance, Attack $f_4(\cdot)$ targets a defined interval $[t_s, t_f]$, where no consumption is reported, simulating a bypass. Other attacks, such as $f_2(\cdot)$ and $f_6(\cdot)$, involve dynamic intervals that vary over time or in response to external factors like tariff fluctuations. These intervals are crucial for accurately simulating real-world energy theft behaviors.

TABLE 3. Summary of simulated electricity theft attacks based on [24].

Attack Type	Attack function
Partial Reduction	$f_1(\mathbf{r}_i[t]) = \alpha \mathbf{r}_i[t]$
	$f_2(\mathbf{r}_i[t]) = \beta[t]\mathbf{r}_i[t]$
	$f_3(\mathbf{r}_i[t]) = \mathbb{E}[\mathbf{r}_i]$
By-pass	$f_4(\mathbf{r}_i[t]) = \begin{cases} 0 & \forall t \in [t_s, t_f] \\ \mathbf{r}_i[t] & \forall t \notin [t_s, t_f] \end{cases}$
By-pass/Partial Reduction	$f_5(\mathbf{r}_i[t]) = \beta[t]\mathbb{E}[\mathbf{r}_i]$
Price-based Load Control	$f_6(\mathbf{r}_i[t]) = \mathbf{r}_i[d - t + 1]$

1) Attack $f_1(\cdot)$: This attack involves reducing the reading $\mathbf{r}_i[t]$ by a constant factor α, where $0 < \alpha < 1$. Uniformly applying this reduction simulates a simple theft through consistent underreporting.
2) Attack $f_2(\cdot)$: This dynamic attack modifies $\mathbf{r}_i[t]$ according to a time-dependent function $\beta[t]$, where $0 < \beta[t] < 1$. This simulates variability in theft, reflecting real-world scenarios where consumption reporting might be intermittently adjusted.
3) Attack $f_3(\cdot)$: This attack reports a daily averaged predicted value $\mathbb{E}[r_i]$ for a fraudulent consumer's consumption, replacing actual readings with a consistent mean value to mask individual spikes or reductions in usage.
4) Attack $f_4(\cdot)$: Known as a bypass attack, it involves the fraudulent consumer reporting zero readings during a defined interval $[t_s, t_f]$, while actual consumption $\mathbf{r}_i[t]$ is reported outside this interval. This simulates

tampering with the meter to display no usage at certain times.

5) Attack $f_5(\cdot)$: Similar to attack $f_3(\cdot)$, this attack utilizes a predicted mean value $\mathbb{E}[r_i]$ for the day's consumption reports. However, unlike $f_3(\cdot)$, it varies the reported value dynamically within the range specified by $\beta[t]$ throughout the day.
6) Attack $f_6(\cdot)$: This attack aims at reducing the electricity bill by reporting low energy consumption during periods of high tariffs and vice versa without changing actual consumption. This method illicitly takes advantage of tariff fluctuations to reduce the overall expense.

4) DATA PRE-PROCESSING

To generate a malicious attack dataset, we initiated the process by first defining the parameters of the electricity theft attack functions. The parameters were set as follows:

1) For the functions $f_1(\cdot)$, $f_2(\cdot)$, and $f_6(\cdot)$, as well as the variables $\beta[t]$ and α, we generated random values uniformly distributed within the interval (0.1, 0.6), in line with the methodologies described in [24].
2) For the bypass attack implemented in $f_4(\cdot)$, the start time t_s was determined using a uniform distribution over the interval $(0, 42)$. The duration of the attack, defined as $t_f - t_s$, was similarly generated as a uniform random variable within the range $(6, 48)$, ensuring the attack's end time t_f could extend up to the maximum of 48.

Upon applying these configurations, the dataset for each smart meter was augmented to include $1 \times 25,728$ genuine records and 6 fabricated attack samples for each day, distributed across the original $25,728$ records. Consequently, for $2,000$ smart meters, the dataset comprises $2,000 \times 25,728$ honest samples alongside $12,000 \times 25,728$ malicious samples, resulting from $6 \times 2,000$ smart meters subject to simulated attacks.

TABLE 4. Optimal hyper-parameters of the neural network models.

Model	2D CNN+	LSTM	FFN	2-D CNN	CONVLSTM
L	**2**	1	2	5	1
D_H	0.5	-	-	0.4	0.2
O	Adam	Adam	Adam	Adam	Adam
A_H	ReLU	tanh	ReLU	ReLU	ReLU
A_O	Sigmoid	Sigmoid	Sigmoid	Sigmoid	Sigmoid
Lr	Schedular	Schedular	0.001	0.001	0.001
Bs	64		64	64	64

5) DATA IMBALANCE

The dataset exhibits a significant imbalance, with malicious samples outnumbering honest samples in a ratio 6:1. To mitigate the challenges posed by this imbalance, we adopt the ADASYN method [50] aimed at equalizing the distribution between the two classes within the dataset, which encompasses $25,728$ honest energy consumption readings for each smart meter. The ADASYN method initiates the rebalancing process by calculating the ratio of the minority class (honest samples) to the majority class (malicious samples).

After implementing the ADASYN approach, the dataset comprises $12,000$ records, each containing $25,728$ electricity consumption readings, balanced between honest and malicious entries. The dataset was subsequently partitioned into three sets: training, validation, and testing, using a distribution ratio of 3:1:1.

6) FEATURE EXTRACTION WITH 2-D CNN AND LSTM

To prepare the data for analysis using our 2-D Convolutional Neural Network (CNN) model, we transformed the consumption readings into a matrix format optimized for weekly analysis. For each customer, the data was reshaped into a weekly record represented by a 7×48 matrix, where the 7 rows correspond to the days of the week, and the 48 columns represent half-hourly consumption readings for each day. Over a period of 536 days, we generated 77 weekly records per customer. This matrix format enables the detection model to analyze the weekly consumption patterns of each smart meter (SM_i).

Upon processing this input through the CNN, a feature map with dimensions $77 \times 7 \times 64$ is produced at the second convolutional layer. This feature map is then input into an LSTM network for further processing. Specifically, the 2-D CNN outputs a feature map sized $M \times N \times G$ ($77 \times 7 \times 64$) after the second convolutional layer, with G representing the number of convolutional maps in the final convolutional layer. Using a time-distributed wrapper, the input to the LSTM layer is reshaped to $M \times NG$ (77×448), reflecting the temporal dimensionality of the data at each specific time point t as illustrated in Figure 5. An LSTM layer is tasked with extracting the $M \times NG$-dimensional vectors, denoted as X_t, at each time step t to enhance model performance. These vectors, termed feature slices X_t, are processed by the LSTM at each time step t to capture temporal dynamics within the data. A detailed discussion of the temporal mechanisms utilized by the LSTM layers is provided in section IV.

C. MODEL HYPERPARAMETERS

Selecting the right model hyperparameters is essential for optimizing the performance of our electricity theft detection model. Table 4 outlines the optimal hyperparameters that were determined through comparative analysis with other architectures, highlighting the configurations that yielded the best results. The chosen hyperparameters include the number of hidden layers (L) $= \{1, 2, 3, 4, 5, 6\}$, the optimizer (O) $= \{$SGD, RMSprop, ADAM$\}$, the dropout rate $(D_H) = \{0.2, 0.4, 0.5\}$, the hidden activation function $(A_H) = \{$ReLU, tanh, linear, sigmoid$\}$, the output activation function $(A_O) = \{$softmax, sigmoid$\}$, the learning rate (Lr) $= \{$softmax, sigmoid$\}$, and the batch size (Bs) $= \{32, 64, 128\}$

TABLE 5. Performance evaluation.

Scheme	Model Structure	DR (%)	FAR (%)	HD (%)	ACC (%)	PR	AUC
Our Scheme	CONVLSTM	**92.95**	**3.68**	**89.27**	**94.65**	**98.80**	**98.50**
Ibrahem *et al.* [12]	FFN	91.30	6.83	84.47	92.21	98.00	97.10
Yao *et al.* [11]	2-D CNN	90.66	12.32	78.34	89.02	96.90	96.00
Gao *et al.* [16]	CONVLSTM	89.22	4.06	85.16	92.39	97.90	97.90

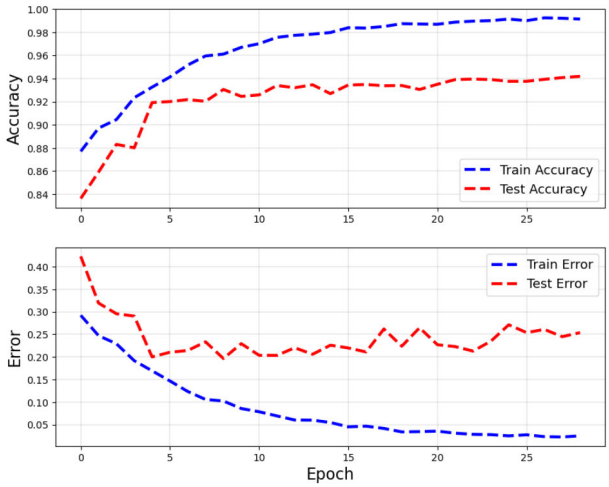

FIGURE 6. Accuracy and loss evaluation for the dataset.

Our model's design includes two 2-D convolutional layers and one LSTM layer, with the convolutional layers using the ReLU activation function for faster training and increased non-linearity. Following the first convolutional layer is a dropout layer with a 40% rate to help prevent overfitting. All weights are initialized using the Glorot method [51], which ensures stable variance of activations and gradients across layers for effective training.

The output layer of the model uses the sigmoid activation function, suitable for binary classification tasks, where 0 denotes normal users and 1 indicates electricity theft. This function is preferred for its output range between 0 and 1. The model uses the Adam optimizer and a learning rate scheduler to adjust the learning rate efficiently during training. To tune the training epochs, the model has been trained with over 30 epochs with a batch size of 64 as depicted in Figure 6 using binary cross-entropy loss function. After 20 epochs, the model's performance on the training data continued to improve slightly, but the performance on the testing data plateaued indicating that the model had effectively learned the underlying patterns.

D. PERFORMANCE METRICS

To evaluate our scheme's performance, we conduct a comprehensive evaluation using a wide range of metrics derived from a confusion matrix. Relying solely on accuracy and loss evaluation metrics is not dependable in measuring the effectiveness of our detection model. The confusion matrix provides insights into the following outcomes.

- True Positive (TP): A benign sample correctly identified as benign.
- True Negative (TN): A malicious sample correctly identified as malicious.
- False Positive (FP): A benign sample incorrectly identified as malicious.
- False Negative (FN): A malicious sample incorrectly identified as benign.

In this study, we use several key performance indicators, including the Detection Rate (DR), False Alarm Rate (FAR), Highest Difference (HD), Accuracy (ACC), Precision-Recall (PR), and Receiver Operating Characteristics (ROC) for the evaluation of our detection model. DR measures the percentage of fraudulent consumers correctly detected as shown in Equation: (13). The FAR measures the percentage of honest consumers falsely recognized as dishonest, as depicted in Equation: (13). The highest difference (HD) between DR and FAR, as given in Equation: (14). Accuracy measures the percentage of honest or fraudulent consumers correctly identified, as shown in Equation (15). Optimal model performance is achieved when DR, HD, and accuracy are high, and FAR is low.

$$DR = \frac{TP}{TP + FN} \quad FA = \frac{FP}{TN + FP} \tag{13}$$

$$HD = DR - FA \tag{14}$$

$$ACC = \frac{TN + TP}{TN + FP + TP + FN} \tag{15}$$

In addition, we have used the ROC curve to illustrate each model detection performance by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR) across different thresholds. The Area Under the Curve (AUC) quantifies the model's ability to differentiate between classes, with a higher AUC indicating better performance. Lastly, the PR curve shows the tradeoff between Precision and Recall for different thresholds. The high AUC represents both high Recall and high Precision, where high Precision relates to a low False Positive Rate, and high Recall relates to a low False Negative Rate.

E. PERFORMANCE EVALUATION

Table 5 presents the detection performance of various deep learning-based classifiers, utilizing the optimal hyperparame-

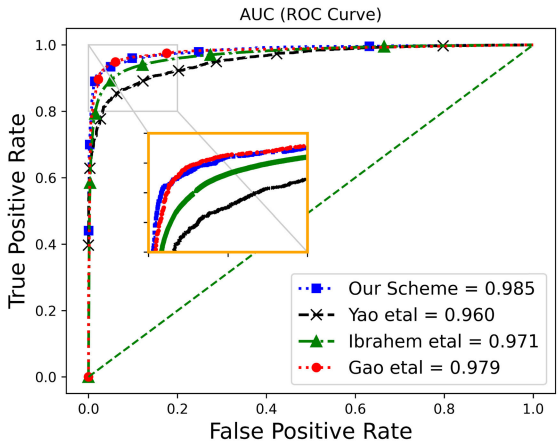

FIGURE 7. ROC curve of different schemes.

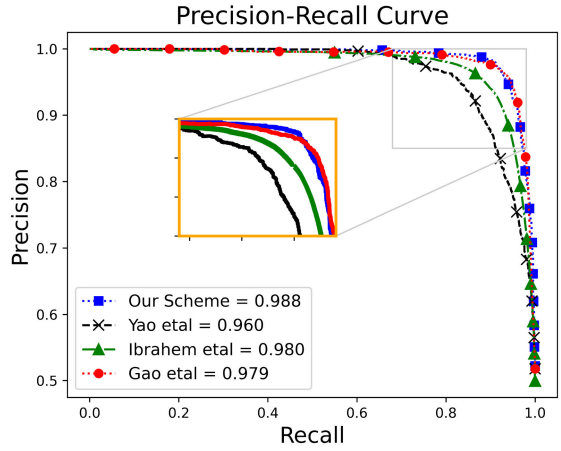

FIGURE 8. PR curve of different schemes.

ters. Our hybrid 2-D CNN-LSTM detector outperforms other architectures in terms of key detection metrics.

Our proposed model demonstrates superior performance, achieving an accuracy of 94.65%, a detection rate (DR) of 92.95%, and the lowest False Alarm Rate (FAR) of 3.68%. In contrast, the FNN model registers an accuracy of 92.21%, a DR of 91.30%, and a FAR of 6.83%. The 2-D CNN models exhibit an accuracy of 89.02%, a DR of 90.66%, and a FAR of 12.32%. Furthermore, the CONVLSTM model shows an accuracy of 92.39%, with a DR of 89.22% and a FAR of 4.06% over 30 epochs. Our detector demonstrates improvements in accuracy (2.29 − 5.63%), DR (1.65 − 3.73%), FAR (0.38 − 8.64%), PR (0.8 − 1.9%) and AUC (0.60 − 2.5%).

The superior performance can be attributed to the integration of 2-D CNN with LSTM, which effectively captures periodic features and temporal correlations within the time-series electricity consumption data. This hybrid architecture ensures robust capabilities in detecting instances of power theft. While some discrepancies between actual and predicted results suggest minimal inaccuracies, these are comparatively negligible when evaluated against the models proposed in [11], [12], and [16]. Notably, the 2-D CNN's detection rate of 90.66% shows a marginal improvement of 1.44% over the CONVLSTM, though it records the highest FAR due to its limitations in capturing sequential patterns in the time-series data.

The ROC curve, illustrated in Figure 7, plots the True Positive Rate (TPR) against the False Positive Rate (FPR) across various thresholds. Our model's ROC curve, characterized by a blue dashed line, achieves an AUC of 0.985, indicating nearly perfect performance in distinguishing between classes. Additionally, the Precision-Recall (PR) curve for our model, shown in Figure 8, summarizes the model's performance across all thresholds. With higher PR values compared to competing models, our scheme indicates better Precision and Recall with an AUC of 0.988, reinforcing its effectiveness in class discrimination.

F. COMPUTATION OVERHEAD

Computation overhead is defined as the processing time required by each entity in the system, KDC, SMs, and EU to run the system initialization, reading encryption, and securely evaluating the first of the detection model respectively. We implemented our scheme, and the proposed schemes in [11] and [12] using the Python Charm cryptographic library [52]. The confidentiality of the power consumption readings in out of the scope of [16] and hence it is excluded from this comparison.

Figure 9(a) shows the computation overhead required by the KDC to run the KeyGen Algorithm vs the of number of the readings to be encrypted in each electricity theft detection period. As shown in the figure, [11] exhibits a fixed time to generate the SM and EU keys. This is because their scheme utilized the well-known Paillier cryptosystem to encrypt all the readings such that only a single public/private key pair is generated and this public key is broadcasted to all the smart meters. On the other hand, our scheme and [12] are constructed based on the principles of IPFE in which the key size is dependent on the readings' vector size. Our scheme is more efficient when compared to [12] because our scheme requires efficient arithmetic operations compared to the computation expensive operations over $\mathbb{G}^2$ and $\mathbb{Z}^2$ used in [12]. Moreover, the scheme in [12] requires the KDC to generate a unique functional decryption key to be used by the EU for each SM, unlike our scheme which utilizes a single functional decryption key for all the users. This will not only increase the linear complexity shown in Figure 9(a) into a quadratic complexity, but also will require a storage overhead at the EU side to store one key per each consumer which seems an unscalable solution.

Figure 9(b) shows the computation cost required by the SM to encrypt all the readings in a single detection period. Our scheme that utilizes the SIP technique, and [12], constructed based on [53] are extremely efficient when compared with [11] since each reading in [11] is encrypted using the Paillier cryptosystem.

The computation overhead at the utility side to evaluate the output of the first layer in the detection model is shown

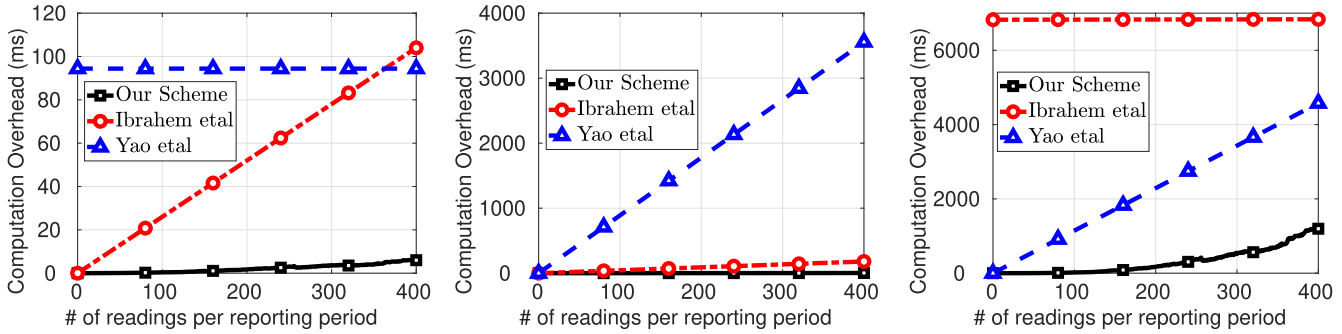

FIGURE 9. Computation overheads comparison.

in Figure 9(c). This is the *most important* overhead since the utility will continuously and repeatedly monitor a large number of consumers at every detection period. Our scheme is the most efficient because the evaluation of this process requires a single dot product operation between the received ciphertext vector $\mathbf{ct}_i$ and the stored functional decryption key $\mathbf{dk}_{\mathbf{w}_{jk}}$ unlike [11] that requires a single decryption operation of the Paillier ciphertext for each reported reading. The scheme in [12] is constructed based on [53] in which the most computationally expensive operation requires solving the discrete logarithmic problem to recover the output of the first layer in the detection model [54]. It should be noted that [11] has a weak threat model because it requires a trusted node to decrypt every single reading and run the detection model over the plaintext reading unlike our scheme and [12] in which the EU runs the detection model using the received encrypted data without violating consumer's privacy.

It should be noted that [11] uses an intermediate node called *server gateway* which is assumed as trusted entity that has access to all the individual power consumption data. Therefore, [11] not only violates the consumers' privacy protection, but also incurs an additional computation overhead, not shown on the figures, that is added by the intermediate node to decrypt each received reading, run the detection model for each reading from each smart meter, and aggregate the electricity theft detection results to send them to the EU.

VII. CONCLUSION

In this paper, we developed a ConvLSTM-based detector that integrates a 2-D privacy-preserving CNN with an LSTM network. This innovative combination effectively extracts high-level features and captures long-term dependencies in power consumption patterns, significantly enhancing detection accuracy. Our approach introduces a novel, general-purpose, and lightweight inner-product functional encryption scheme, based on the secure inner product using linear invertible matrices. This scheme allows the secure computation of the convolution process over encrypted 2D data without revealing the content of the data, hence ensuring data confidentiality. Our security analysis demonstrates that the proposed scheme can ensure the power consumption data confidentiality and hence, ensure the consumer's privacy. Our scheme achieves a superior Detection Rate (DR) of 92.95%, a False Alarm Rate (FAR) of 3.68%, and a High Detection (HD) rate of 89.27%, resulting in an overall Accuracy (ACC) of 94.65%. In addition, our scheme achieves high Precision (PR) at 98.80% and a robust Area Under the Curve (AUC) value of 98.50%. Furthermore, the computation costs incurred by our scheme are minimal, making it highly suitable for real-time applications. These results demonstrate that our scheme not only achieves high detection accuracy, but also is extremely efficient for the secret key generation, data encryption, and secure convolution computation which makes it an efficient and practical solution in problems where running CNN-based model over encrypted data is necessary.

ACKNOWLEDGMENT

The authors would like to acknowledge the Alabama Power and Mobility (AMP) Center support in conducting this work. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF or AMP.

REFERENCES

[1] A. A. Esmael, H. H. da Silva, T. Ji, and R. da Silva Torres, "Non-technical loss detection in power grid using information retrieval approaches: A comparative study," *IEEE Access*, vol. 9, pp. 40635–40648, 2021.

[2] N. Kebir and M. Maaroufi, "Technical losses computation for short-term predictive management enhancement of grid-connected distributed generations," *Renew. Sustain. Energy Rev.*, vol. 76, pp. 1011–1021, Sep. 2017.

[3] Z. Yan and H. Wen, "Performance analysis of electricity theft detection for the smart grid: An overview," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–28, 2022.

[4] H. Fang, J.-W. Xiao, and Y.-W. Wang, "A machine learning-based detection framework against intermittent electricity theft attack," *Int. J. Electr. Power Energy Syst.*, vol. 150, Aug. 2023, Art. no. 109075.

[5] T. Ahmad, H. Chen, J. Wang, and Y. Guo, "Review of various modeling techniques for the detection of electricity theft in smart grid environment," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 2916–2933, Feb. 2018.

[6] A. Alsharif, M. Nabil, S. Tonyali, H. Mohammed, M. Mahmoud, and K. Akkaya, "EPIC: Efficient privacy-preserving scheme with EtoE data integrity and authenticity for AMI networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3309–3321, Apr. 2019.

[7] BBC News, "Smart meters can be hacked to cut power bills," 2014. Accessed: Jul. 4, 2024. [Online]. Available: https://www.bbc.com/news/technology-29643276

[8] 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.

[9] 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.

[10] Electronic Privacy Information Center. *The Smart Grid and Privacy*. Accessed: Apr. 8, 2019. [Online]. Available: https://epic.org/privacy/smartgrid/smartgrid.html

[11] 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.

[12] 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.

[13] X. Feng, H. Hui, Z. Liang, W. Guo, H. Que, H. Feng, Y. Yao, C. Ye, and Y. Ding, "A novel electricity theft detection scheme based on text convolutional neural networks," *Energies*, vol. 13, no. 21, p. 5758, Nov. 2020.

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

[15] Z. Xia, D. Yin, K. Gu, and X. Li, "Privacy-preserving electricity data classification scheme based on CNN model with fully homomorphism," *IEEE Trans. Sustain. Comput.*, vol. 8, no. 4, pp. 652–669, 2023.

[16] H.-X. Gao, S. Kuenzel, and X.-Y. Zhang, "A hybrid ConvLSTM-based anomaly detection approach for combating energy theft," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–10, 2022.

[17] *Cer Smart Metering Project—Electricity Customer Behaviour Trial 2009–2010*, Commission for Energy Regulation (CER), Ireland, 2012.

[18] M.-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.

[19] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1830–1837.

[20] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids: A P2P computing approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 257–267, Sep. 2013.

[21] S.-C. Yip, C.-K. Tan, W.-N. Tan, M.-T. Gan, and A. A. Bakar, "Energy theft and defective meters detection in AMI using linear regression," in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur.*, Jun. 2017, pp. 1–6.

[22] S. Salinas, C. Luo, W. Liao, and P. Li, "State estimation for energy theft detection in microgrids," in *Proc. 9th Int. Conf. Commun. Netw. China*, Aug. 2014, pp. 96–101.

[23] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, Apr. 2013, pp. 57–64.

[24] 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.

[25] 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.

[26] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[27] 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.

[28] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[29] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[30] N. Duan, C. Huang, C.-C. Sun, and L. Min, "Smart meters enabling voltage monitoring and control: The last-mile voltage stability issue," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 677–687, Jan. 2022.

[31] M. Orlando, A. Estebsari, E. Pons, M. Pau, S. Quer, M. Poncino, L. Bottaccioli, and E. Patti, "A smart meter infrastructure for smart grid IoT applications," *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12529–12541, Jul. 2022.

[32] S. I. Gerasopoulos, N. M. Manousakis, and C. S. Psomopoulos, "Smart metering in EU and the energy theft problem," *Energy Efficiency*, vol. 15, no. 1, Jan. 2022. [Online]. Available: https://link.springer.com/article/10.1007/s12053-021-10011-y

[33] A. Graves and J. Schmidhuber, "Framewise phoneme classification with bidirectional LSTM networks," in *Proc. IEEE Int. Joint Conf. Neural Netw.*, vol. 4, Jul. 2005, pp. 2047–2052.

[34] S. Sharma, S. Sharma, and A. Athaiya, "Activation functions in neural networks," *Towards Data Sci.*, vol. 6, no. 12, pp. 310–316, 2017.

[35] M. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. M. Islam, and J.-M. Kim, "Electricity theft detection in smart grid systems: A CNN-LSTM based approach," *Energies*, vol. 12, no. 17, p. 3310, Aug. 2019.

[36] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory Cryptography*. Berlin, Germany: Springer, Mar. 2011, pp. 253–273.

[37] S. Agrawal, B. Libert, and D. Stehlé, "Fully secure functional encryption for inner products, from standard assumptions," in *Advances in Cryptology—CRYPTO 2016*. Berlin, Germany: Springer, Jul. 2016, pp. 333–362.

[38] M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval, "Simple functional encryption schemes for inner products," in *Public-Key Cryptography—PKC 2015*. Berlin, Germany: Springer, Mar. 2015, pp. 733–751.

[39] C. Baltico, D. Catalano, D. Fiore, and R. Gay, "Practical functional encryption for quadratic functions with applications to predicate encryption," in *Advances in Cryptology—CRYPTO 2017*. Cham, Switzerland: Springer, Jul. 2017, pp. 67–98.

[40] M. Nabil, A. Alsharif, A. Sherif, M. Mahmoud, and M. Younis, "Efficient multi-keyword ranked search over encrypted data for multi-data-owner settings," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[41] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[42] A. Sherifl, A. Alsharif, M. Mahmoud, M. Abdallah, and M. Song, "Efficient privacy-preserving aggregation scheme for data sets," in *Proc. 25th Int. Conf. Telecommun. (ICT)*, Jun. 2018, pp. 191–195.

[43] A. Alsharif, M. Nabil, A. Sherif, M. Mahmoud, and M. Song, "MDMS: Efficient and privacy-preserving multidimension and multisubset data collection for AMI networks," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10363–10374, Dec. 2019.

[44] A. Sherif, A. Alsharif, M. Mahmoud, and J. Moran, "Privacy-preserving autonomous cab service management scheme," in *Proc. 3rd Afr. Middle East Conf. Softw. Eng.*, Dec. 2017, pp. 19–24.

[45] M. Nabil, A. Sherif, M. Mahmoud, A. Alsharif, and M. Abdallah, "Efficient and privacy-preserving ridesharing organization for transferable and non-transferable services," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1291–1306, May 2021.

[46] R. Mutegeki and D. S. Han, "A CNN-LSTM approach to human activity recognition," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 362–366.

[47] A. Alsharif, M. Nabil, M. M. E. A. Mahmoud, and M. Abdallah, "EPDA: Efficient and privacy-preserving data collection and access control scheme for multi-recipient AMI networks," *IEEE Access*, vol. 7, pp. 27829–27845, 2019.

[48] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *Proc. ACM SIGMOD Int. Conf. Manage. data*, Jun. 2009, pp. 139–152.

[49] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: When QoE meets QoP," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 74–80, Aug. 2015.

[50] 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.*, Jun. 2008, pp. 1322–1328.

[51] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proc. 13th Int. Conf. Artif. Intell. Statist.*, 2010, pp. 249–256.
[52] 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.
[53] S. Agrawal, B. Libert, and D. Stehlé, "Fully secure functional encryption for inner products, from standard assumptions," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2016, pp. 333–362.
[54] J. Klesczewski, "Combinatorial and stochastic approach to parallelization of the kangaroo method of solving the discrete logarithm problem," M.S. thesis, Rochester Inst. Technol., Rochester, NY, USA, 2021.

JOHNSON ANIN received the B.S. degree in electrical and electronic engineering from the University of Mines and Technology, Ghana, in 2017, the M.S. degree in electronics engineering from Norfolk State University, Norfolk, VA, USA, in 2020, and the Ph.D. degree in electrical and computer engineering from The University of Alabama (UA), Tuscaloosa, AL, USA, in August 2024. He is an Instructor with the Department of Physics & Astronomy and the Department of Electrical Engineering, UA. His research interests include security and privacy in smart grids, machine/deep learning, hardware, and software engineering.

MUHAMMAD JAHANZEB KHAN received the bachelor's degree in computer science from the NFC Institute of Engineering and Technology, Pakistan, the master's degree in computer science from the University of Nevada Reno, Reno, NV, USA, and the master's degree in software engineering from Shanghai Jiao Tong University, China. He is currently pursuing the Ph.D. degree with The University of Alabama, Tuscaloosa, with a focus on AI, federated learning, and privacy preservation. He is also a Computer Science Scholar. His research interests include deeply rooted in leveraging AI for societal benefit, with notable contributions to federated learning and privacy-preserving technologies. He actively engages in the Linux community, demonstrating his passion for open-source initiatives and collaborative innovation.

OMAR ABDELSALAM received the bachelor's degree in computer science with a focus on data science and artificial intelligence, along with a minor in mathematics from Tennessee Technological University (TNTech), in 2024, where he is currently pursuing the Ph.D. degree in large language models. During his undergraduate years, he engaged in extensive research and internships, including a notable research experience for undergraduates (REU) with The University of Alabama, where he worked on building encryption schemes and deep learning techniques to enhance the security of machine learning models. He has co-authored several publications in major IEEE conferences and journals, such as the IEEE INFOCOM Conference and IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS. His research interests include large language models, reinforcement learning, and the security of machine learning models. He has also been active in academic and professional communities, serving as the Vice President for the MSA Students' Association at TNTech and holding multiple leadership positions.

MAHMOUD NABIL (Senior Member, IEEE) received the B.S. and M.S. degrees (Hons.) in computer engineering from Cairo University, Egypt, in 2012 and 2016, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, Cookeville, TN, USA, in August 2019. He is an Associate Professor with the Department of Electrical and Computer Engineering, North Carolina A&T State University. He is an accomplished Researcher. He has received significant funding for his research projects from esteemed national agencies and organizations, including the National Science Foundation (NSF), the Department of Transportation (DOT), the Air Force Research Laboratory (AFRL), NASA, Intel, Cisco, and Lockheed Martin. He has authored or co-authored several publications in prestigious venues. His research has been published in renowned journals, such as IEEE INTERNET OF THINGS, IEEE TRANSACTIONS OF DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON HUMAN–MACHINE SYSTEMS, and IEEE TRANSACTIONS OF MOBILE COMPUTING. He has also contributed to leading conferences, including the International Conference on Communication, International Conference on Pattern Recognition, and International Conference on Wireless Communication. With diverse research interests, his areas of expertise include security and privacy in unmanned aerial systems, smart grids, machine learning applications, vehicular ad hoc networks, and blockchain applications.

FEI HU (Member, IEEE) received the first Ph.D. degree in signal processing from Tongji University, Shanghai, China, in 1999, and the second Ph.D. degree in electrical and computer engineering from Clarkson University, New York, NY, USA, in 2002. He is currently a Professor with the Department of Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL, USA. His research has been supported by U.S. NSF, DoE, DoD, Cisco, and Sprint. He has published over 200 journal/conference papers and book (chapters) in the field of wireless networks and machine learning. His research interests include wireless networks, machine learning, big data, and network security and their applications.

AHMAD ALSHARIF (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in electrical engineering from Benha University, Cairo, Egypt, in 2009 and 2015, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, Cookeville, TN, USA, in May 2019. Currently, he is an Assistant Professor with The University of Alabama, Tuscaloosa, AL, USA. He also holds the position of an Assistant Professor with the Faculty of Engineering at Shoubra, Benha University, Egypt. His research interests include applied cryptography, secure protocol design, IoT security, cyber-physical systems security, and the use of machine learning in cybersecurity. In 2022, he received the U.S. National Science Foundation Research Initiation Initiative Grant (NSF CRII); and the Young Innovator Award from the Egyptian Industrial Modernisation Center, in 2009.