Generative Edge Intelligence for Securing IoT-assisted Smart Grid against Cyber-Threats

Gopal Chaudhary, Smriti Srivastava, Manju Khari

[1] VIPS-TC, School of Engineering & Technology, New Delhi, India
[2] School of Computer and System Sciences, Jawaharlal Nehru University, New Delhi-67
[3] Netaji Subhas University of Technology, New Delhi,
Emails: gopal@vips.edu; manjukhari@jnu.ac.in; smriti.nsit@gmail.com

Abstract
The critical dependence of industrial smart grid systems on cutting-edge Internet of Things (IoT) technologies has made these systems more susceptible to a diverse array of assaults. This consequently puts at risk the integrity of energy data as well as the safety of energy management activities that depend on those data. This study offers a generative federated learning framework for semi-supervised threat detection in an IoT-assisted smart grid system. We refer to this framework as FSEI-Net. A unique semi-supervised edge intelligence network (SEI-Net) is presented in the FSEI-Net to enable semi-supervised training using labeled and unlabeled data in the edge tier. The design of SEI-Net is based on with bidirectional generative convolutional network that can intelligently capture the patterns of threat data from partially labeled smart grid data. We present federated training to enable remote edge servers to work together on training a semi-supervised detector without disclosing their own private local data. This is accomplished through cooperative training. To facilitate communication between cloud and edge layers that is both secure and respectful of users' privacy, a reputation-based block chain is introduced in the FSEI-Net. The outcomes from the practical applications demonstrate that the effectiveness of the proposed FSEI-Net over the most recent cutting-edge detection approaches are valid.

Keywords: Industrial Smart Grid; Federated Learning; Energy Protection; Attack Detection.

1. Introduction

THE transition from traditional industrial power systems to industrial smart grids has been facilitated by ongoing developments in the internet of things (IoT) and wireless communication technologies. This gives the industrial smart grid system an even greater ability to maximize the efficiency of energy distribution and provide excellent administration facilities [1]. Cyber-physical systems, also known as CPSs, are frequently used in the construction of smart grid networks. These systems combine the physical and digital worlds in order to improve the quality of service (QoS) provided by smart grid applications [2]. The CPSs include the following three categories of component parts: The material parts that come together to form the smart grid system for industrial use (i.e., electricity generator, motors, controllers, etc.). The cyber components are not directly connected to the real world in any way. The physical and digital worlds are brought together by the cyber-physical components, which consist of the devices that make this connection [2]. The emergence of a cyber-physical smart grid has been offering many benefits to the energy community, such as improved energy loss mitigations, increased reliability, enhanced power superiority, and cost optimization [1-3].

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

Widespread use of smart grid technology has brought about two-way communication between smart meters and utility suppliers; as a result, the electricity providers are able to make load adjustments dynamically based on the users' actual consumption data, thanks to the information provided by smart meters. Now more than ever, a variety of nations and businesses are advocating for the installation of smart meters. By the year 2023, more than 200 million homes in Europe will be equipped with smart electricity meters, making the total number of smart meters in Europe 200 million [2]. Nevertheless, the vast number of smart meters that are being deployed presents a possible threat to individuals' privacy. Transmissions made by a smart grid include data on instantaneous electricity consumption in addition to data on other topics. The research presented in [3]–[5] demonstrates that it is feasible for an adversary to obtain people's private information by intercepting the immediate electricity usage data. These advanced strategies were demonstrated in the work of [3]–[5].

Since real-time power utilization, information could expose some behavioral information about individuals or organizations, this information can be very revealing. As a result, preventing the disclosure of the real-time consumption data of users is an absolute necessity. In addition, the vast majority of them can prevent the disclosure of customers' real-time energy utilization data. This has been done so that users' privacy may be protected. Nevertheless, some setups only allow one data type to be transmitted from smart meters to the service provider. This is insufficient when the utility company wants to conduct a thorough analysis of the data on electricity consumption. In addition, the method of verifying messages in some schemes is inefficient, and it takes a considerable amount of time to complete the verification process. This study demonstrates that the identity-based signature technique can significantly speed up the verification process.
The communication of industrial smart grid components and IoT devices at various industrial smart grid nodes leads to more complex smart grid systems with a massive amount of data [4]. This data could be utilized for system management, consumption monitoring, and energy measurement analysis. Despite this, the excessive dependence of industrial smart grid applications on IoT makes them more susceptible to a wide variety of security flaws and malicious attacks with the ability to cause damaging cyber or physical consequences [2, 5]. There are two different types of assaults that can be launched against the industrial smart grid system. To begin, we will define physical attacks as those that result in the overt modification of physical components. Second, malicious software or gaining access to the individual components of an industrial smart grid system are the two most common ways that cyber threats are carried out [3]. Existing security solutions are unable to fulfill their intended function inside a smart grid environment. For instance, the use of access control and encryption methods could potentially disrupt analytical skills and lead to an increase in the number of false alarms [2]. The industrial smart grid system is vulnerable to both passive and active attacks, the former of which seeks to collect the original power data and the latter of which seeks to change it [7]. As a result, this could pose a significant risk to the data integrity and, therefore, have a detrimental effect on the performance of any data-driven analytics [6]. Therefore, a reliable threat detection mechanism that is driven by data is necessary for ensuring both the security and privacy of data in industrial smart grid systems and the IoT networks that they are connected to [1].

Deep learning, also known as DL, has been shown to be an effective data-driven analytical method in IoT networks. For instance, convolutional neural networks (also known as CNNs) have shown impressive performance in feature extraction [1]. Recurrent models, such as recurrent neural networks (RNNs), long short-term memory (LSTM) [2, and gated recurrent units (GRU) [3] are having a lot of impact due to their capacity to learn and discern temporal relations in IoT data. On the other hand, these models are unable to fulfill the requirement of real-time threat detection in an environment with limited labeled data and constrained resource availability. In light of this, the authors of this study propose a brand new lightweight, semi-supervised deep learning architecture for threat detection, with the end goal of enabling reliable energy management within an industrial smart grid system.

There has been a lot of focus on privacy protection (PP) in the Internet of Things (IoT) settings in recent years. However, many obstacles have not been thought of yet. Here, differential privacy (DP), homomorphic encryption (HE), and authentication protocols (AP) make up the backbone of the currently available PP methods. With the goal of keeping sensitive information about businesses off the smart grid, researchers have shown a lot of interest in the DP method [4]. The DP methods introduce random noise into the power data, typically using a Gaussian and/or Laplace distribution. The generation and utilization of noise values are useful and efficient. On the other hand, it severely hampers data use and the efficacy of smart grid operations in the industry. In addition, the HE methods use remote computers to do the necessary calculations on the encrypted data [5]. However, HE is unfit to manage real-time industrial smart grid applications because of the significant requirement for processing resources during

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

encryption and decryption operations. In addition, AP methods have traditionally depended on either a global key cryptosystem, a hashing process, or a signature value [6]. Provide simple and effective privacy solutions but can only compute simple accumulation methods securely and cannot support complex operations [7]. In light of the importance of detecting cyber threats in Cloud-Edge-assisted industrial smart grid systems, this research provides a unique blockchain-enabled federated learning (FL) framework.

The rationale for this research is based on the essential security needs for the design of dependable energy management in industrial smart grids, which are as follows:

- There is also the issue of security to consider since the transmission of power demands and supply to and from cloud servers is a necessary part of central control of the industrial smart grid system.
- Energy providers are wary of sending data through IoT networks to a cloud server due to worries about data privacy because many industrial smart grid applications deal with highly confidential information.
- Since labeling industrial smart grid data is a time-consuming and labor-intensive operation, only a small fraction of the data is on the process of tagging, while a substantial volume of unlabeled data is typically available. As a result, it gets harder to use annotated and unannotated data for distributed learning.

This study contributes to fulfilling the before mentioned research gaps as follows:

- This study presents a new semi-supervised Edge Intelligence Network (SEI-Net) that promotes collaborative detection of different intrusions and anomalies for distributed edge nodes in the smart grid environment. The proposed FSEI-Net is dependent on training information, making it scalable; it does not depend on system specifications or topological features of the underlying IoT network.
- Unlike supervised approaches, the employed semi-supervised FSEI-Net enables robust attack detection using a tiny amount of annotated data and a bigger capacity of unannotated data, which empowers the network to generalize well on unseen data samples.
- A blockchain tier with an improved Proof-of-Stake (PoS) reputation-based consensus strategy is introduced to safeguard the privacy of data and model parameters in the industrial smart grid system.

The following is how the remainder of this work is scheduled to be completed: In the next section, we will discuss the relevant literature. The model of the proposed system is shown in Section III. In Section IV, we will talk about how the FSEI-Net framework was designed. In Section V, we talk about how the experiment was set up. The following section, Section VI, presents the findings and then discusses them. Finally yet importantly, the study is finished with a succinct summary in Section VII, which also discusses potential next steps.

I. Related Works

Several recent publications have used either federated or centralized deep learning methods to tackle the problem of cyber threats in IoT-based smart grids. In this section, we review the related literature under two types of threat intelligence methods, namely supervised methods, and semi-supervised ones. Then, we review the edge intelligence for smart grid applications.

A. Supervised Threat Intelligence

Detecting threats in IoT environments is a hot research topic that attracted the attention of the research community in recent times. The work [1] developed a unique federated DL model for hunting cyber threats against container-based industrial edge computing systems which were demonstrated to have flexible deployment nature as well as adequate resource orchestration [2]. The work tried to efficiently detect attacks in smart transportation using federated FL approaches that shift the burden of training from central servers to vehicular edge nodes, on which context-aware transformer model was presented for identifying specific types of attacks, FED-IDS implemented a. it applied block chain-managed federated training, which uses decentralized ledger technology to make it possible for a network of edge nodes to provide trustworthy, dispersed, and secure education [3]. The work [4] surveyed the literature on threat intelligence approaches by taxonomizing the criminal behaviors, indicators, and risk characteristics that can be employed for these approaches. it also surveys the most pressing engineering and managerial concerns and factors. More, to detect attacks in IIoT data flow, the work [5] presented a forensics-based DL model that incorporated an MHA layer to record and learn global representations, and it learns local interpretations using local GRU. However, those threat intelligence frameworks also struggle with performance issues when dealing with Big IIoT traffic data generated by IIoT devices due to their lack of scalability [6], [7], [8]. To get over the lack of structure in cyber threat intelligence and get at the tactics, techniques, and procedures, the

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

work [9] presented an attention-based methodology named the Attention-based Transformer Hierarchical Recurrent model that was built with many steps. The first step is the development of a Transformer Embedding Architecture (TEA) for acquiring comprehensive semantic information on threat intelligence. Then, it developed an Attention Recurrent Structure (ARS) to process culminates in the creation of a unified hierarchical classification module, which can be used to foretell the ultimate tactics, techniques, and Procedures.

B. Semi-supervised Threat Intelligence

The complexity of annotating big-enough cyber threat data has motivated a lot of researchers to explore the adoption of unlabeled data in their threat intelligence models. For example, The work [10] presented a semi-supervised threat intelligence framework that is built up with multiscale temporal convolution operations as well as intelligence traffic attention to effectively extract threat patterns from IoT flows. It also presented a hierarchical semi-supervised learning scheme to empower the network to keep historical retraining during the learning from IoT traffic. More, the research presented in [11] a unique federated semi supervised generative network for detecting abnormal power data in micro grids supported by the edge, while improving the superiority of generating minority samples and interactions between labeled and unlabeled data. In this work, both the generator and the discriminator to boost the representation power during training, making the two components block-structured, use temporal convolutions.

C. Edge Intelligence

Edge intelligence is the use of AI-powered gadgets and systems located close to the point of measurement to perform tasks such as data gathering, storage, computing, and analytics. When it comes to data and user security, edge intelligence is all about protecting both. In spite of its relative youth (2011-present), this area of study has shown phenomenal expansion during the past years [12]. The work [13] reviewed the state of the art in current EI studies in detail. To be more specific, we first recap the history and justification for AI deployments at the network's periphery. Then, it summarized the current state of the art and future directions of major technologies for training and inferencing deep learning models at the network's periphery. The work [14] developed a methodology that makes supervised learning techniques at the edge easier to implement. In particular, it breaks down elaborate models into a series of simpler classifiers. This was evaluated in the context of human activity recognition by contrasting the results obtained with a variety of distinct implementations of this approach.

2. System model

The architecture of our system is primarily composed of three primary tiers, which are as follows: the cloud Backend, the edge computing tier, and the block chain tier.

D. Cloud Backend

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

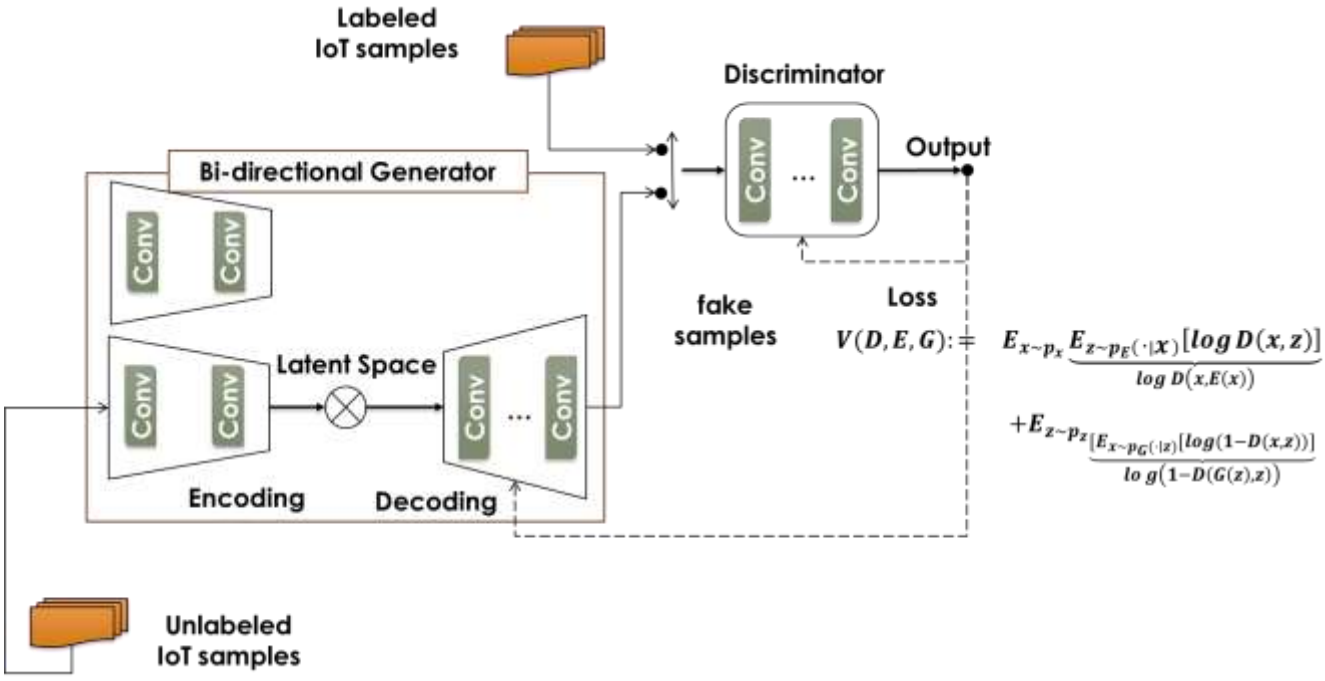

Figure 1: The architecture of the proposed SEI-Net.

It is the responsibility of the cloud tier to put together a complete FSEI-Net framework by federating and then updating the parameters of the locally trained model that is stored on edge devices. Multiple communication rounds between the cloud server and the participating edge nodes, with the goal of semi-supervised cooperatively training them with the corresponding private data (see section IV). In addition, the management of the request-supply cycle is often the responsibility of the cloud tier in a smart grid system.

E. Edge Network

The servers are computational entities that are taking part in the training of FSEI-Net. They are responsible for distributing remote computing resources to end devices and bringing them closer together. More specifically, after the cloud has scheduled the participating nodes, the deployer will then deploy the container images that arrive from the code fountain, will run the threat detector, and will finally deliver the results back to the Edge nodes. In order to reduce the amount of time spent in broadcast dormancy, the edge devices use a direct route to connect with the SMART GRID nodes. FSEI-Net is also expandable and adaptable, as the edge servers can be enthusiastically connected or withdrawn by the cloud manager based on physical constraints or health circumstances. This allows FSEI-Net to accommodate a growing number of users.

F. Blockchain network

The FSEI-Net framework makes use of blockchain technology to operate as a distributed archive for documenting and authenticating transactions that take place within the framework. A threat intelligence hash and an associated data hash are both required components of a transaction. Additionally, the personalities and keys of presenting edge nodes, as well as the accomplishment moment, are also required. In order to facilitate the decentralized members' ability to move forward and scrutinize threat intelligence operations, the proposed FSEI-Net cultivates four smart contracts. 1) Identity Contract (IC): This protocol provides the core manipulation activities necessary for storing the credentials of decentralized ESs and Edge nodes. 2) Upload Contract (UC): This contract verifies the personalities of Edge nodes and ESs by communicating with the IC, and then it uploads the required operations to the blockchain network. Credit Contract (CC): It ensures that the status of each decentralized participant is kept intact. 3) Voting Contract (VC): It is responsible for nominating the members of the confederation and initiating examinations for electing on transactions. After that, it will ask the CC to use blockchain tokens to reward or punish members according to how truthful or fraudulent they have been.

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

The following are the stages that are involved in the VC process: 1) a value chosen at random is generated after each round and used as the seed for the voting process, which results in an increased level of safety; 2) Each member calls Verifiable Random Functions (VRF) to produce an arbitrary number depending on the seed and status rate; 3) An arbitrary numbers that were generated are sorted in descending order, and f members of the consortium are picked for voting on the legality of the transactions. After the edge servers have completed the semi-supervised training, they will compile the necessary resources and evoke the UC to add the transactions to the block chain. The Identity Contract will then be invoked to validate the credentials, and the relevant data will then be added to the block chain. Because of this, transactions, including vital data, can be recorded in the distributed ledger and validated by scattered edge servers.

Members of this network resort to VC in order to approve financial dealings among themselves. When a deal has a public vote of approval, it is generally accepted [15] [16]. If a dishonest user's actions are discovered and judged inappropriate, the system will notify CC to deduct assets from their block chain account as a form of punishment. The throughput of current block chain systems is observed to be low, at around seven transactions per second [15] [16]. The FSEI-Net uses an enhanced Proof-of-Stake (PoS) reputation-based consensus strategy to address this concern. To what extent may far distant nodes acquire a stellar reputation, and what opportunities exist for them to mine blocks and join them to the block chain's upper layer. The FSEI-Net contacts the CC to improve the standing of all users. As a result, the throughput FSEI-Net is increased without the need for the time-consuming process of Bitcoin. But if nodes are incentivized to be trustworthy by contributing their computing power to transaction validation, then the Proof-of-Stake approach could be a viable option. Therefore, the technique improves the block chain's bandwidth and safety. As a whole, [18] proved that our architecture could withstand the misbehavior of geographically distant adversaries. Consequently, the use of the block chain provides an additional layer of security and reliability for FSEI-Net, and businesses can reliably take part in the smart grid system [17].

II. PROPOSED FSEI-NET

This portion of the paper primarily argues the design of the *SEI-Net* architecture and the way the convolutions are leveraged to capture the threat representations in the smart grid data, as shown in Fig. 1. Besides, we explain how labeled and unlabeled data fed to the *SEI-Net* for semi-supervised training with accelerated loss calculation to offer a real-time security solution for smart grid applications. Finally, the federated training for the SEI-Net model in a privacy-preserving cloud-edge architecture.

A. Semi-supervised Edge Intelligence Net (SEI-Net)

Utilizing the properties of IoTs that are related to network traffic, we construct threat intelligence using a generative adversarial network (GAN). The Nash equilibrium is where the fundamental concept of GAN originates from. It is made up of a generator, G, and a discriminator, D, when it comes to game models that involve two different players. The generator will first determine the possible distribution of actual data examples, and then it'll generate new training datasets based on that information. The discriminator, on the other hand, is comprised of two classifiers that differentiate between the input data and the output data. Players in two games need to consistently optimize and develop their own production and discriminating capabilities if they hope to emerge victorious from the contest. The objective of this step of learning and optimizing is to locate a Nash equilibrium between the two players. GAN is a two-player game that has no winner and no loser. The aggregate of the stakes held by both participants remains unchanged.

For its data generation, GAN makes use of adversarial approaches; an explanation of the method's fundamental operation may be found in Fig. 1. The process of creating a hostile network is similar to playing a combat game. Finding new opponents to spar with on a regular basis and gaining experience via these fights is the best way to develop your fighting abilities and is an essential part of the learning process. The following value function, $V(G,D)$, is one way to define GAN:

$$\min_G \max_D V(G,D) = E_{\boldsymbol{x}\in p_{data}(\boldsymbol{x})}\left[lo\, g\left(D(\boldsymbol{x})\right)\right] + E_{\boldsymbol{z}\in p_{\boldsymbol{z}}(\boldsymbol{z})}\left[lo\, g\left(1-D\left(G(\boldsymbol{z})\right)\right)\right] \quad (1)$$

In the above formula, the symbol E signifies the anticipation function, while D *and* G are implemented with any stack of DL layers. $p_{data}(\boldsymbol{x})$ and $p_{\boldsymbol{z}}(\boldsymbol{z})$ correspond to input IoT batch and noise terms, correspondingly. Thus, $\boldsymbol{x}$ and $\boldsymbol{z}$, respectively, represent the traffic samples as well as noise vectors. Backpropagation (BP) is a technique that can be employed to modify the variables of a GAN model. This algorithm takes into account the objective functions of

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

both discriminatory and generator models. With the help of the gradient BP algorithm, the GAN parameters are able to be determined accurately. Because of this, the strategy that is based on GAN is the one that we employ to address the matter of threat detection. The generator picks example z from the noise distribution $p_z(z)$. Accordingly, the fabricated information is outputted by the generator, which is denoted by $G(z)$, where the differential convolutional functions are adopted to implement the architecture of the generator. In this scenario, the discriminator D reads the input $p_{data}(\boldsymbol{x})$ and determines that it contains the example x.

$$E_{\boldsymbol{x}\in p_{data}(\boldsymbol{x})} log\left(F\left(D(\boldsymbol{x})\right)\right). \quad (2)$$

The function $F\left(D(\boldsymbol{x})\right)$ represents the output of D which is a real number in the interval [0-1]. The Discriminator's normal-value prediction accurateness is maximized according to eq.(2), such that:

$$F\left(D(\boldsymbol{x})\right) = 1 \; if \; \boldsymbol{x} \in p_{data}(\boldsymbol{x}), \quad (3)$$

Then we check the generator's output, that is

$$E_{\boldsymbol{z}\in p_z(\boldsymbol{z})} log\left(1 - F\left(D\left(G(\boldsymbol{z})\right)\right)\right). \quad (4)$$

Maximizing the aforementioned formula G is unable to produce high-quality fraud data. The generator's job is to produce bogus information that could trick the discriminator. Thus, the discriminator of SEI-Net seeks to optimize the following formula:

$$\max_D E_{\boldsymbol{z}\in p_z(\boldsymbol{z})}[log\left(1 - D\left(G(\boldsymbol{z})\right)\right] + E_{\boldsymbol{x}\in p_{data}(\boldsymbol{x})}[log\left(D(\boldsymbol{x})\right)]. \quad (5)$$

SEI-Net updates the network architecture to be conditioned to some class label. In particular, the generator G is informed to produce an artificial sample for a particular class of threat data, which is defined by label$y$. This implies updating the fitness function as follows:

$$\min_G \max_D V(G,D) = \min_G \max_D E_{\boldsymbol{x}\sim p_r}[log\, D(\boldsymbol{x}|\boldsymbol{y})] + E_{\boldsymbol{z}\sim p_z}\left[log\left(1 - D\left(G(\boldsymbol{z}|\boldsymbol{y})\right)\right)\right] \quad (6)$$

The symbol y denotes the one-hot code of the particular threat category. It is worth noting that the CGAN shares similar training with GAN. Jensen-Shannon (JS) deviation is used as the measure for synthesizing examples for both networks, which leads to issues including modal breakdown and training inconsistency. As a remedy, the vanishing of gradients during GAN and CGAN training was addressed by updating the design of SEI-Net to follow the design of Wasserstein GAN, which in turn demonstrated an efficient solution for the issues of modal breakdown. To better approximate reality, SEI-Net replaces the JS divergence used to compute the loss function with the Wasserstein distance, commonly known as the Earthmover (EM) distance, which is described as sees:

$$EM(p_r, p_g) = \inf_{\gamma\in\prod(p_r,p_g)} E_{(\boldsymbol{x},\boldsymbol{y})\sim\gamma}[\|\boldsymbol{x} - \boldsymbol{y}\|] \quad (7)$$

This way, the SEI-Net is optimized by the following function:

$$\min_G \max_D V(G,D) = \min_G \max_D E_{\boldsymbol{x}\sim p_r}[D(\boldsymbol{x})] - E_{\boldsymbol{z}\sim p_z}[D\left(G(\boldsymbol{z})\right)] \quad (8)$$

Beyond, the SEI-Net innovatively combined the advantages of EM distance and CGAN into a bidirectional design of generator and discriminator, to create multiple latent representations of the input data. The encoder took in all features and produced their latent representation of size 16 and the generator produced generated network data from the noise z of the same size as the latent representation.

The SEI-Net can be trained to optimize the following cost function:

$$\min_{G,E} \max_D V(D,E,G) \quad (9)$$

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

$$V(D,E,G):= E_{x\sim p_x}\underbrace{E_{z\sim p_E(\cdot|x)}[log\ D(x,z)]}_{log\ D(x,E(x))} + E_{z\sim p_z}\underbrace{[E_{x\sim p_G(\cdot|z)}[log(1-D(x,z))]}_{log(1-D(G(z),z))} \quad (10)$$

Given the above formulation, the design of the encoder-decoder part in the proposed SEI-Net is trained according to mean square loss:

$$L^R = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - G\left(E(z_i)\right)\right)^2, \quad (11)$$

Whilst the cross entropy function is adopted for optimizing the discriminator:

$$L^D = -\sum_{c=1}^{M} y_c\, log(p_c) \quad (12)$$

Whereas y_c and p_c denote the actual class as well as the predicted one, respectively.

B. *Federated training*

The vital idea behind the FSEI-Net framework is to enable multiple distributed edge servers to collaboratively train a global semi-supervised threat detector without revealing their private. To realize this, a federated training scheme is introduced to train the proposed SEI-Net employed together with a block chain-protected cloud-edge architecture. The first phase of training includes the initialization procedures for the main components of the FSEI-Net framework as follows. A secure block chain channel is introduced for reliable and privacy-preserving communications between the cloud tier and edge tier. Besides, the cloud tier set the initial parameters of the FSEI-Net in terms of batch-size $B = 32$, the learning rate $\alpha = 0.005$, the number of epochs (i.e., 90 epochs), the number of edge nodes (i.e., 20 nodes), and the percentage of labeled and unlabeled data at each participating edge server. In addition, an iterator variable r represents the number of communications rounds between an edge node and a central cloud server.

Then, the contributing edge server initializes its local models based on cloud initialization, and then starts training the local SEI-Net using the $loss^{final}$ly. Once the local training is completed, all edge nodes push up the recomputed local gradient to the cloud tier through the block chain channel to guarantee that unreliable participants cannot poison the training process. Following this, the cloud tier aggregates the local gradients and recomputed the global gradient, and then the global gradient is broadcasted back to the local SEI-Net. This process is repeated for each communication around until the final global gradient is returned.

III. EXPERIMENTAL DESIGN

A. *Data Description*

To experiment with the proposed FSEI-Net framework for smart power networks, we used the datasets NSL-KDD [18] and UNSW-NB15 [19]. The former data is an enhanced edition of the KDDCUP99, which exemplifies 63 days of unrefined TCP abandon traffic streams of a local-area network (LAN) imitating the standard Air Force LAN in the united states. The LAN has functioned like an actual Air Force system, influenced by unauthorized access to local super user with root privileges (U2R) attacks, unauthorized access from a remote machine (R2L) attacks, Denial-of-Service (DoS) attacks, and surveillance and other probing attacks [18]. The data is spitted into 125,973 training samples and 22,544 test samples. The latter dataset contains a mixture of 42 variables for standard and malicious recordings, which corresponds to nine attack categories of data including DoS, exploits, worms, shellcode, reconnaissance, generic, backdoor, analysis, and fuzzes. It consists of 42 attributes. The data spitted into 175,341 training samples and 82,332 test samples.

B. *Performance measures*

For evaluating the performance of the FSEI-Net framework, accuracy, and f1-score are employed and are defined by the following formulas.

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (13)$$

$$Precision = \left(\frac{TP}{TP + FP}\right) \times 100 \quad (14)$$

$$Recall = \left(\frac{TP}{TP + FN}\right) \times 100 \quad (15)$$

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (16)$$

Where TP, TN, FP, and FN represent the true positive samples, true negative samples, false positive samples, and false negative samples, respectively.

C. *Implementation setup*

The simulation experiments are conducted on a Dell personal computer that is equipped with a graphical processing unit of NVIDIA RTX, CPU of Intel (R) Xeon (R) CPU E5-2670 0@ 2.60GHz, a RAM of 48GB, 64-bit windows 10 as an operating system. The coding of the methods is done using the PyTorch library deployed on Python 3.7.1. Twenty laptops with the same designs are implemented as edge devices, which are connecting over a wireless link. Distinctly, each edge server is equipped with four cored Intel(R) Xeon(R) E5-2670 0 2.6GHz CPU and 2GB memory.

IV. Results and Discussions

This subsection provides the results of evaluating the proposed SEI-Net under centralized training on the cloud or federated training in cloud-edge architecture. This experiment is performed with 20% of data labeled with no adversary included. It could be noted that the proposed FSEI-Net realizes robust detection performance with a small performance drop compared with the centralized SEI-Net for both datasets. Moreover, the performance of the two architectures is compared with recent competing semi-supervised approaches i.e., GAN [20], and AE [21]. The results presented in Table I demonstrated the efficiency of the SEI-Net with great performance improvements (Accuracy: 1%-3%, F1 score 2%-4%). This can explain the effectiveness of leveraging the convolutions in modeling the temporal representation in GAN architecture.

Table 1: comparative analysis of the proposed FSEI-Net against cutting-edge models.

	NSL-KDD		UNSW-NB15	
Model	Accuracy (%)	F1-score (%)	Accuracy (%)	F1-score (%)
AE [21]	76.91	74.31	78.82	76.02
GAN[20]	79.13	76.87	80.64	78.34
SEI-Net	82.35	81.14	82.31	80.72
FSEI-Net	80.94	80.06	80.09	79.26

This subsection evaluates the proposed FSEI-Net when implemented with $Loss^D$only, $Loss^R$ only, and a combination of them. Fig. 2 shows the results of these experiments on both datasets. It could be observed that using $Loss^R$ resulted in the lowest performance for both datasets. In contrast, the usage of attaining $Loss^D$only attained great performance improvements (Accuracy: 8%-9%, F1 score 9%-12%). Compared with $Loss^D$scenario, the integration of both loss functions results in 3% and 2% of performance improvements in accuracy and f1-score, respectively. Moreover, to investigate the impact of the amount of labeled data included for training, the proposed FSEI-Net has experimented with different percentages of labeled data and the corresponding result for each experiment is presented in Table II. It is important to note that expanding the amount of labeled data is more favorable for the detection rate. This is because it provides more supervising at the miner, which helps minimize the related loss and increases productivity as a result.

Table 2: Analysis of the effect of the amount of labeled data on FSEI-Net.

Percentage	NSL-KDD		UNSW-NB15	
	Accuracy	F1-score	Accuracy	F1-score

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

	(%)	(%)	(%)	(%)
10%	79.13	77.17	78.67	76.34
20%	80.94	80.06	80.09	79.26
30%	82.35	81.14	81.28	80.84
40%	84.94	83.27	84.08	82.25
50%	89.13	85.24	86.93	84.04

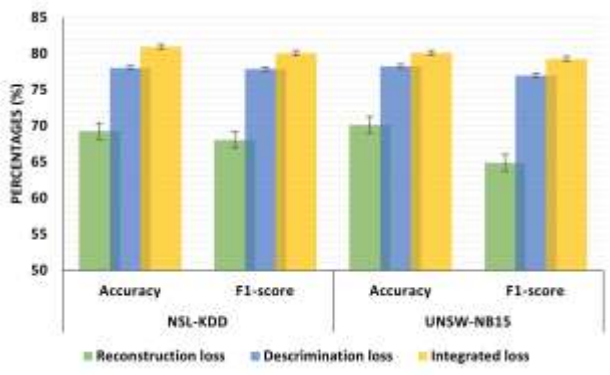

Figure 2: The accuracy of FSEI-Net under different loss functions

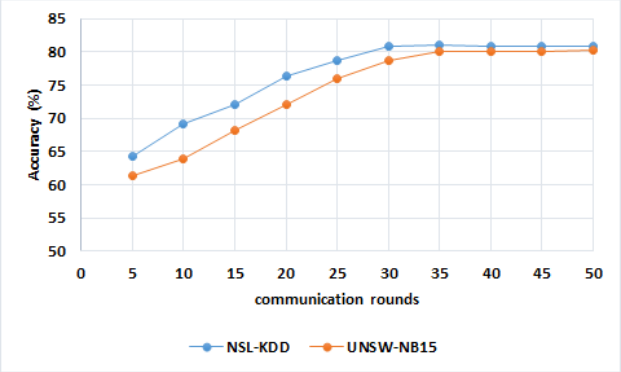

Figure 3: The accuracy of FSEI-Net under various rounds

Moreover, we experiment performance of FSEI-Net under various numbers of cloud-edge communication rounds when trained on the two datasets, as shown in Fig. 3. It could be seen that the detection performance is stabilized after 30 and 35 rounds of cloud-edge communications for NSL-KDD and UNSW-NB15 respectively. The number of rounds is almost equal for all two datasets indicating rapid convergence. This can be justified by the effectiveness of modeling temporal representations during the mapping of data to latent feature space using the proposed encoder network. Further, Fig. 4 shows the detection results of the proposed FSEI-Net under a different number of adversaries ranging from 0 to 5 ($Ad^0, \cdots, Ad^5$) for the two datasets. Where Ad^0 indicates no adversary. It could be noted that detection performance slightly declined with the increase in the number of adversaries. This is because the block chain tier prevents malicious entities from participating in the training process. The incurred marginal decrease came from the decrease in the number of participants. Furthermore, Fig. 5 shows the detection performance of the proposed FSEI-Net under the different number of participating edge servers. These experiments are performed by setting a single edge node as an adversary. It is observable that a smaller number of participating edge nodes results in lower detection performance as the adversary might poison a larger proportion of the data. In contrast, higher detection performance is attained by increasing the number of participating edge nodes, which implies a smaller proportion of data is poisoned by the adversary.

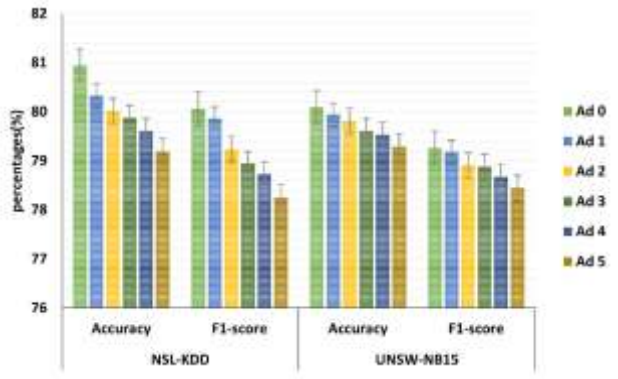

Figure 4: The performance of the FSEI-Net under different numbers of adversaries

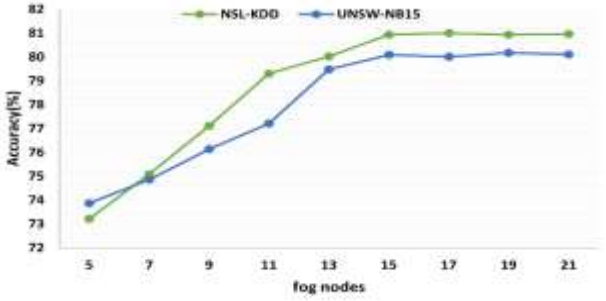

Figure 5: The accuracy of FSEI-Net under different numbers of fog nodes

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

3. Conclusion

This study offers an FL framework (i.e., FSEI-Net) for detecting attacks in a cloud-edge-assisted smart grid system. The FSEI-Net comprises two main tiers: a contributor tier and a cloud tier. Where the attackers employ GAN models to initiate adversarial instances and injects them into the dataset of each smart grid system. The Cloud tier controls the federated training of distributed *SEI-Net* models to precisely identify a malevolent model and remove the contaminated experiments. The findings of thorough experiments validated that our methods outperform existing competing schemes in terms of detection accuracy. Future research directions could include extending the proposed FSEI-Net to consider analyzing the abnormal behavior of new and undetectable attacks. In addition, an improved aggregation method might be researched to enhance the FL approaches in the smart grid system.

References

[1] M. Abdel-Basset, H. Hawash, and K. Sallam, "Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System," *IEEE Trans. Ind. Informatics*, 2022, doi: 10.1109/TII.2021.3091150.

[2] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, and G. Srivastava, "P2TIF: A Blockchain and Deep Learning Framework for Privacy-Preserved Threat Intelligence in Industrial IoT," *IEEE Trans. Ind. Informatics*, 2022, doi: 10.1109/TII.2022.3142030.

[3] W. Zhang, Y. Bai, and J. Feng, "TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT," *Futur. Gener. Comput. Syst.*, 2022, doi: 10.1016/j.future.2022.02.023.

[4] G. Cascavilla, D. A. Tamburri, and W. J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers and Security*. 2021, doi: 10.1016/j.cose.2021.102258.

[5] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2020.3025755.

[6] M. van Haastrecht *et al.*, "Correction: van Haastrecht et al. A Shared Cyber Threat Intelligence Solution for SMEs. Electronics 2021, 10, 2913," *Electronics (Switzerland)*. 2022, doi: 10.3390/electronics11030349.

[7] M. van Haastrecht *et al.*, "A shared cyber threat intelligence solution for smes," *Electron.*, 2021, doi: 10.3390/electronics10232913.

[8] S. Gong and C. Lee, "Cyber threat intelligence framework for incident response in an energy cloud platform," *Electron.*, 2021, doi: 10.3390/electronics10030239.

[9] C. Liu, J. Wang, and X. Chen, "Threat intelligence ATT&CK extraction based on the attention transformer hierarchical recurrent neural network," *Appl. Soft Comput.*, vol. 122, p. 108826, Jun. 2022, doi: 10.1016/j.asoc.2022.108826.

[10] M. Ebrahimi, J. F. Nunamaker, and H. Chen, "Semi-Supervised Cyber Threat Identification in Dark Net Markets: A Transductive and Deep Learning Approach," *J. Manag. Inf. Syst.*, 2020, doi: 10.1080/07421222.2020.1790186.

[11] Y. Li, J. Li, and Y. Wang, "Privacy-Preserving Spatiotemporal Scenario Generation of Renewable Energies: A Federated Deep Generative Learning Approach," *IEEE Trans. Ind. Informatics*, 2022, doi: 10.1109/TII.2021.3098259.

[12] D. Xu *et al.*, "Edge Intelligence: Empowering Intelligence to the Edge of Network," *Proc. IEEE*, 2021, doi: 10.1109/JPROC.2021.3119950.

[13] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," *Proc. IEEE*, 2019, doi: 10.1109/JPROC.2019.2918951.

[14] O. Gomez-Carmona, D. Casado-Mansilla, D. Lopez-De-Ipina, and J. Garcia-Zubia, "Optimizing Computational Resources for Edge Intelligence Through Model Cascade Strategies," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3118845.

[15] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE Internet Things J.*, vol. XX, no. X, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3025916.

[16] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," *IEEE Trans. Ind. Informatics*, 2020, doi: 10.1109/TII.2019.2938001.

[17] S. Rathore and J. H. Park, "A Blockchain-based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, 2020, doi: 10.1109/tii.2020.3040968.

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022

[18] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," 2009, doi: 10.1109/CISDA.2009.5356528.

[19] N. Moustafa, B. Turnbull, and K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2018.2871719.

[20] Y. Zhang, J. Wang, and B. Chen, "Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach," *IEEE Trans. Smart Grid*, 2021, doi: 10.1109/TSG.2020.3010510.

[21] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *J. Netw. Comput. Appl.*, 2020, doi: 10.1016/j.jnca.2020.102767.

DOI: https://doi.org/10.54216/IJWAC.060104
Received: October 12, 2022 Accepted: November 23, 2022