Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs

Partha S. Sarker, *Student Member, IEEE,* Sajan K Sadanandan, *Member, IEEE*,
Anurag K. Srivastava, *Fellow, IEEE,*

***Abstract*—The electric grid operation is constantly threatened with natural disasters and cyber intrusions. The introduction of Internet of Things (IoTs) based distributed energy resources (DERs) in the distribution system provides opportunities for flexible services to enable efficient, reliable and resilient operation. At the same time, IoT based DERs comes with cyber vulnerabilities and requires cyber-power resiliency analysis of the IoT-integrated distribution system. This work focuses on developing metrics for monitoring resiliency of cyber-power distribution system, while maintaining consumers' privacy. Here, resiliency refers to the system's ability to keep providing energy to the critical load even with adverse events. In the developed cyber-power Distribution System Resiliency (DSR) metric, the IoT Trustability Score (ITS) considers the effects of IoTs using a neural network with federated learning. ITS and other factors impacting resiliency are integrated into a single metric using Fuzzy Multiple-Criteria Decision Making (F-MCDM) to compute Primary level Node Resiliency (PNR). Finally, DSR is computed by aggregating PNR of all primary nodes and attributes of distribution level network topology and vulnerabilities utilizing game-theoretic Data Envelopment Analysis (DEA) based optimization. The developed metrics will be valuable for i) monitoring the distribution system resiliency considering a holistic cyber-power model; ii) enabling data privacy by not utilizing the raw user data; and iii) enabling better decision-making to select the best possible mitigation strategies towards resilient distribution system. The developed ITS, PNR, and DSR metrics have been validated using multiple case studies for the IoTs-integrated IEEE 123 node distribution system with satisfactory results.**

***Index Terms*—Resiliency, Distribution System, IoTs, Cyber-power Modeling of IoTs, Unsupervised Neural Network, Federated Learning, Fuzzy MCDM, DERs, Game Theory, DEA.**

I. Introduction

DISTRIBUTION automation and grid modernization is leading evolution to a cyber-power distribution system [1], [2]. Automation has led to a more efficient and flexible power distribution system, driven by advanced communication infrastructure and digital devices for significantly improved system measurement, computation, and control [3], [4].

With increasing IoT-based intelligent devices, the distribution system is becoming more adaptable and flexible. IoTs are now evolving to the Internet of Everything, as it incorporates and build a system that includes wireless networks, sensors, cloud servers, analytics, smart devices, and advanced technologies. IoTs have been forming a regime that consists of millions of intelligent devices connected to analyze and influence our day-to-day activities [5]–[7]. IoTs record one of the fastest growth rates in computing technologies, with an estimation of 5.3 billion global Internet users and more than three times the global population of devices connected by the year 2023 [8]. As the grid becomes more connected, computations and data managements are increasingly moving to the devices at the network edge. Encouraged by availability, latency, and privacy issues, IoT devices can now perform local computations on these data to provide services to the users without transferring any personal data to a central server, thereby improving privacy. The IoTs help deploy these devices, many of whom can perform local computations on data they hold to provide services to end-users. In particular, IoTs can provide connectivity between distributed energy resources (DER) along critical energy supply corridors and within groups of vital facilities, accommodating privacy concerns and constraints of availability and increasing system resiliency. Recent cyberattacks on the power grid have been of increasing complexity and intricacy, thereby adding to the various threats faced by the power grid. It is essential that the power grid remains resilient to such threats and supply power to the critical loads when subjected to various stress levels. Considering that these risks cannot be eliminated, resiliency becomes vital to enable the essential infrastructure to continue to perform when faced with such threats. In 2017, the National Academy of Sciences, Engineering, and Medicine (NASEM) released a report titled ”Enhancing the Resiliency of the Nation's Electricity System,” [9] which, among other recommendations [10], details the need for defining resilience metrics that can drive planning and operational decisions. There are few works related to resiliency metrics for microgrids without IoTs [11], [12], which are limited in scopes and not applicable for advanced cyber-power distribution systems with IoTs. Therefore, the main focus of this work is to develop holistic cyber-power resiliency metrics by leveraging the ubiquitous presence of IoTs to facilitate an operational solution for both cyber and physical events.

The increasing use of IoT devices in any system brings many other concerns like data integrity, data privacy, data quality, and network communication latencies. When it comes to cyber-power resilience analysis for distribution system planning and operational decisions in the presence of IoT devices, the concerns mentioned above are very critical to address. Various literature approaches use machine learning to tackle these concerns [13], [14] in different systems. But, in general, infrequent communications of most IoT devices in distribution systems make it harder to get enough data points

This work is supported by the Department of Energy under Award DE-OE0000920.

The authors are with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506 USA (e-mail: anurag.srivastava@mail.wvu.edu).

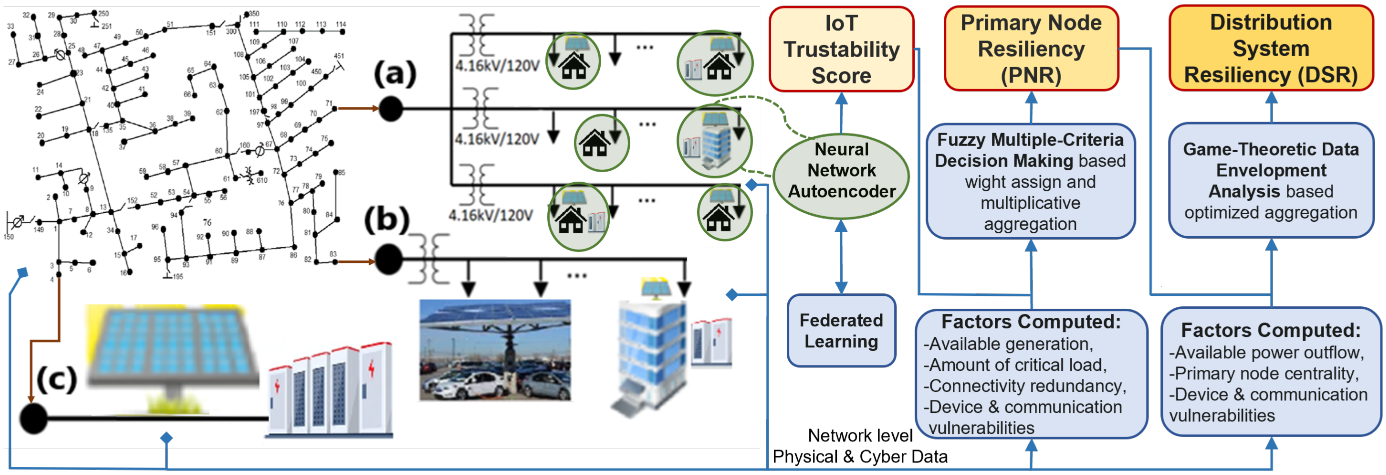
(a)
(b)
(c)
4.16kV/120V
4.16kV/120V
4.16kV/120V
IoT Trustability Score
Primary Node Resiliency (PNR)
Distribution System Resiliency (DSR)
Neural Network Autoencoder
Fuzzy Multiple-Criteria Decision Making based wight assign and multiplicative aggregation
Game-Theoretic Data Envelopment Analysis based optimized aggregation
Federated Learning
Factors Computed:
-Available generation,
-Amount of critical load,
-Connectivity redundancy,
-Device & communication vulnerabilities
Factors Computed:
-Available power outflow,
-Primary node centrality,
-Device & communication vulnerabilities
Network level Physical & Cyber Data

Fig. 1. Overview of the Proposed Resiliency Metrics for Cyber-Power Distribution System with IoTs.

to generate an accurate model of them. Federated learning (FL) architecture can overcome the challenges with data scarcity of these IoTs and generate effective models to enable intelligent applications for systems with IoTs [15]–[18].

Therefore, in this work, we have started with analyzing the distribution system with IoTs and modeled the cyber-power system along with IoTs to better understand the overall changing behaviors of the distribution system. Then, we identified the cyber-power features of IoTs presented in the distribution grid and applied appropriate unsupervised machine learning and federated learning architecture to identify anomalies and formulate IoT Trustability Score (ITS). This approach helps us tackle data scarcity and allows us to protect user data privacy by not bringing the raw user data out of the privacy-protected area. The ITS and all other cyber-physical factors from the secondary level feeder are combined using F-MCDM and multiplicative aggregation to calculate primary level node resiliency (PNR). Finally, overall distribution system resiliency is formulated utilizing game-theoretic-DEA-based optimized aggregation of PNR of all the primary nodes and factors of distribution level network topology and its vulnerabilities.

The key contributions of this work are summarized below:

- Modeled, simulated and analyzed cyber-power distribution system with the IoTs.
- Developed IoT Trustability Score for enhanced monitoring of IoTs using unsupervised neural network model and the federated learning architecture.
- Developed Primary level Node Resiliency metric with Fuzzy Multi-Criteria Decision Making considering IoTs.
- Developed formulation for cyber-power Distribution System Resiliency with Primary level Node Resiliency and attributes from the physical and cyber network using game-theoretic Data Envelopment Analysis based optimized aggregation,
- Validated the developed resiliency metrics through case studies for the IEEE 123 node distribution system with the IoTs.

II. Modeling and Analysis of Cyber-Power Distribution System with IoTs

With the modernization of the power system, distribution systems are also going through significant changes. More and more smart devices and appliances are based on IoTs are replacing traditional distribution system loads [19], [20]. DERs in distribution systems are also utilizing the IoT platform [21]. All these phenomenons are causing significant changes in any distribution system, and further study of distribution systems with IoTs is required to understand these changes. To address this scenario, we have proposed an architecture to compute resiliency metrics for cyber-power distribution systems with IoTs as shown in Fig. 1.

A. Distribution Power System IoTs

According to the IEEE IoT Initiative, IoTs should have features like identity, sensing/actuation capability, embedded intelligence, programmability, and communication capability using internet infrastructure [22]. The initiative also points towards the necessities of application system-specific features when it comes to analyzing that system with IoTs.

The IoT applications in the power system primarily utilize the unique address of IoTs for Transmission Control Protocol (TCP) and Internet Protocol (IP) based communications, comprehensive sensing and intelligent processing features [23]–[25]. Since resiliency focuses on supplying power to the critical loads, characteristics of IoTs associated with power generation and load components are of more interest here.

Therefore, any device with the following attributes are considered as IoTs and included in the modeling and analysis of the distribution system with IoTs for this study:

- Connected to others and can exchange information.
- Has unique identifier like IP address.
- Act as a power source or load.
- Has computing capability.
- Has some autonomous activity.
- Plug & Play.

Following the above discussion, we have considered heating, ventilation, air conditioning (HVAC), solar PV, battery storage, and electric vehicle (EV) as IoTs of interest for this study as they are a significant part of the changing distribution power system.

B. Distribution System Analysis with IoTs

The changing distribution system can be modeled from the primary level node to the secondary level downstream users since most IoTs are deployed from the primary level to downwards. Let consider the IEEE 123 test feeder system as shown in Fig. 1 where three representative primary nodes are expanded to their secondary level. The primary level nodes of this system can be modeled into three categories based on the configuration of each primary level node downstream.

1) Physical Power Primary Node: Though the modernization of the distribution system is going everywhere, there are still some feeders with the legacy connection type. This type of feeder has no digital component in the secondary level downstream, and every operation done here is manual in type.

2) Cyber-Power Primary Node without IoTs: This category covers any primary Node with digital devices but no IoT devices in the secondary level downstream. Digital relays, circuit breakers, switches, etc., are there in the secondary level feeder.

Expanded primary node (a) in Fig. 1 without the PV, battery, and other IoTs, resembles the typical configuration of these two type nodes from the primary level to its downstream.

3) Cyber-power Primary Node with IoTs: IoTs such as HVAC, PV, energy storage, EV, etc., exist downstream of this kind of primary node. This type of node can have three types of feeder configuration in terms of connectivity. They are-

- *Type-A:* Feeders connecting individual buildings/houses with IoTs where the utility does not have access within the buildings/houses as shown in expanded primary node (a) Fig. 1,
- *Type-B:* Feeders connecting large buildings with IoTs such as roof-top PV, building energy storage, EV charging parks where the utility has access as shown in expanded primary node (b) Fig. 1,
- *Type-C:* Big PV farms, energy storage type IoTs are directly connected at the primary voltage level, and there is no secondary level as shown in expanded primary node (c) Fig. 1.

C. Power System Modeling in Gridlab-D

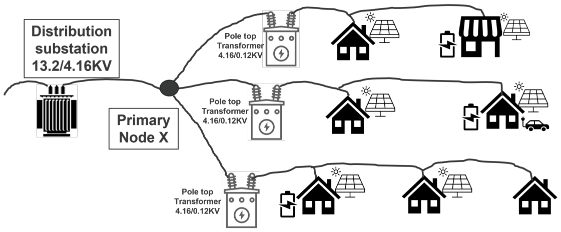
Distribution substation 13.2/4.16KV
Primary Node X
Pole top Transformer 4.16/0.12KV
Pole top Transformer 4.16/0.12KV
Pole top Transformer 4.16/0.12KV

Fig. 2. Secondary level of a typical distribution system.

In order to do a cyber-power simulation of distribution system with IoTs, we have built a typical secondary level feeder from a primary level node 'X' as shown in Fig. 2 in Gridlab-D [26]. A total of six houses and one commercial building are considered. Here, all of them are equipped with normal loads and HAVC. Five houses have solar PV, two houses have battery storage, one house has an EV, and the commercial building has battery storage and solar PV.

Gridlab-D simulation can include real-world climate data in the simulation. Here, all the individual houses and buildings have their own schedule for different common loads that vary from time to time. The house class in Gridlab-D is utilized for both.

EV does not have any model in Gridlab-D yet, so we have considered it a constant load that only turns on at night for charging. This overall Gridlab-D simulation provides all the necessary data which can be easily used to determine the behavior of the power system part of the IoTs.

D. IoT Network Emulation in MININET-WIFI

For cyber network emulation of power systems, Mininet SDN network emulator is commonly used for cyber-power co-simulation [27], [28]. In this work, we are using MININET-WIFI [29], which is a fork of the Mininet. For four IoTs considered in this work, we have created four virtualized wifi stations and connected them to an access point. All of these are based on the standard Linux wireless drivers and the 80211_hwsim wireless simulation driver. For emulating the IoTs operation, we have developed applications that mimic general operations of sensing, calculating, and exchanging information for each IoT device. Now, we run the EMS/IoT Hub application in the access point. We run device-specific applications in the wifi station for each type of device for each IoT. This application reads the data generated by the specific device in the Gridlab-D simulation, represented by the IoT wifi station. We utilize client-server-based communication settings to exchange customized network packets encapsulating the device data generated by Gridlab-D and any instruction from the IoT Hub that communicates to the user via the internet. Fig. 3 shows overall network. We have captured IoTs network traffic through this emulation and utilized different traffic features for ITS formulation.

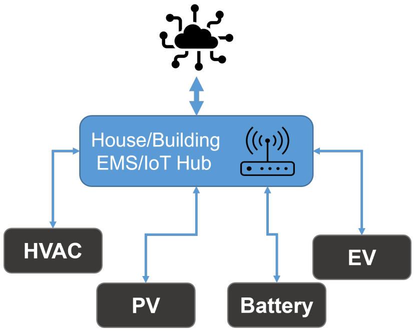

Fig. 3. Building/house IoT network emulation with MININET-WIFI network emulator.

III. IoT Trustability Score (ITS) Formulation using Federated Learning

Monitoring and operating a resilient power system require data from all over the system, including the users. With the increasing amount of data utilization for the operation and control purpose of the distribution system, the risk of exposing users' valuable data is also increasing. While more data helps utilities operate better, this leads to privacy concerns. So, in scenarios where data privacy is required, data use needs to be done in a secure way that will provide the highest possible data utilization for monitoring and control purposes while maintaining privacy. Uses of IoT devices in secondary feeders of the distribution system as shown in Fig. 1 fall under this type of scenario. Again, typically these IoT devices only initiate communication to update about sensor readings and during interactions related to user commands which are also few and far between. As a result, they do not generate enough data to train an accurate model covering all IoT devices' behaviors. A federated self-learning architecture can overcome this limitation of data points for training accurate models while keeping the IoT device data inside any privacy-protected area such as buildings, houses, etc.

We have formulated an ITS utilizing the federated self-learning architecture in this work. Here, IoT cyber network data and the power system data associated with the IoT are considered in this formulation.

ITS provides an insider view of the operating status of IoTs without accessing raw user data. Anomalies in IoTs data are the main factor in formulating the ITS. At first, IoTs network packets were studied for feature selections. The features for all types of devices, IoTs network packet features will be the same. Then features from the specific power system simulation data have been selected to be used for the specific device. More details of the features are shown in Table I.

TABLE I
Features considered for each type of data

Data Source	Features
IoTs network packet	Source/Destination IP, Source/Destination port, Packet length, Protocols, Intra-packet arrival time
HVAC	Timestamp, Load, Indoor temperature, outdoor temperature, Temperature setpoint, Indoor area, Building thermal insulation
PV	Timestamp, Power generation, Rating, Solar irradiance
Battery	Timestamp, Charging/Discharging rate, SoC, KW capacity
EV	Timestamp, Charging rate, SoC

A. Overview of Federated Learning

The Federated Learning architecture generally consists of a curator or server that sits at its center and coordinates the training activities. Here, buildings/houses are considered as clients who have IoT devices. The clients communicate at first with the server to receive the current global model weights of each IoT device and the communication they have from the server. Then they train it on each of their local device data to generate updated parameters for that device model and upload it back to the server for aggregation.

Let's assume there are M clients. Then, utilizing the concept of Federated Averaging Algorithm [30], if the clients estimate their weight parameters W_i^t for minimum reconstruction error (RE) for each type of IoT device, we can scale all clients weight parameters and sum to get the final global weight W_G for each type of IoT devices as shown in (1).

$$W_G = \sum_{i=1}^{M} \frac{n_i}{n} W_i^t \tag{1}$$

Where, n_i is the number of data points in client i for one data type, and n is the total data point which is the sum of the number of data points of that type of data of all M clients. An overview of federated learning is shown in Fig. 4.

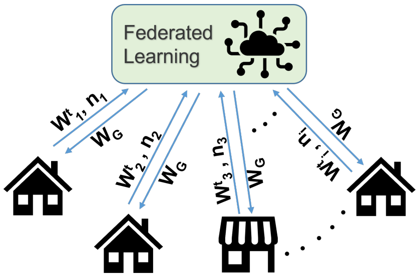

Fig. 4. An overview of federated learning.

B. Autoencoder for Unsupervised Learning

An unsupervised autoencoder neural network is used for the local training part of the federated learning architecture. Autoencoder is very useful for anomaly detection in cyber-power systems, especially with unlabeled data [31], [32]. Autoencoder efficiently captures the correlations and interactions between the various variables by compressing the data to a lower-dimensional representation for complex data. The autoencoder model minimizes the RE during training, which is the mean squared distance between input and output. In this work, an autoencoder neural network model is built utilizing Keras module [33] in python and modified to be used in federated learning architecture. The optimized model is constructed with five fully connected hidden layers with 6, 3, 2, 3, 6 neurons. The neuron number of the input and out layer depends on the data feature number.

C. ITS Formulation

The overall formulation of the ITS is shown in Fig. 5. The federated learning explained above is applied here for each type of data. For each client, there will be one autoencoder model for each IoT device to train on its power system data and one more autoencoder model to train only on IoT network packet data. During the training session, each client's IoT devices are closely monitored to ensure that the client trains the IoT network packet autoencoder model with normal network data and their device-specific autoencoder models with device-specific power system normal data received via

IoT network packet communication. Once all the clients go through the federated learning process for each IoT device and receive the global weight parameter W_G for all the autoencoder models, the monitoring session starts.

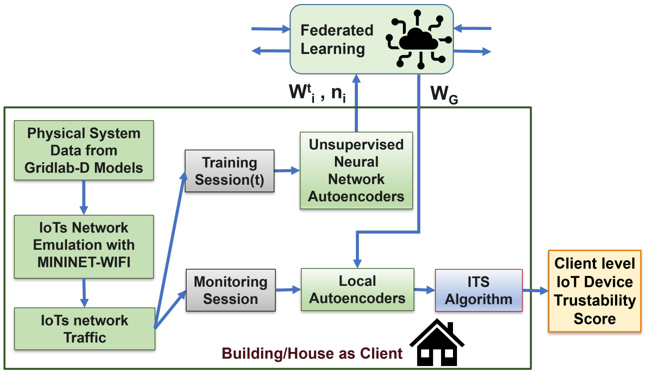
Federated Learning
W^t_i , n_i
W_G
Physical System Data from Gridlab-D Models
Training Session(t)
Unsupervised Neural Network Autoencoders
IoTs Network Emulation with MININET-WIFI
Monitoring Session
Local Autoencoders
ITS Algorithm
Client level IoT Device Trustability Score
IoTs network Traffic
Building/House as Client

Fig. 5. An Overview of implementation of IoT Trustability score formulation.

First, for each type of data, each client calculates RE values for their own training data points at their local autoencoder block with the global weight parameter W_G and sends it to ITS Algorithm block to decide on a tolerance value T_{err} for the RE. ITS Algorithm block selects the maximum RE value as T_{err}. Then each client monitors all the network packet and power system data of each of its IoT devices and reconstructs them using the global weight parameter W_G in the local autoencoders block.

ITS Algorithm block flags any data point as an anomalous data point (ADP) if the data point (DP) crosses T_{err}. Then, for any reporting time period Δt, non-anomaly ratio (NAR) is calculated using,

$$NAR = 1 - \frac{\text{Total ADP number over } \Delta t}{\text{Total DP number over } \Delta t} \tag{2}$$

Now, the ITS Algorithm block calculates the cumulative non-anomaly ratio ($CNAR$) to capture behaviors of the IoTs for some most recent time periods. $CNAR$ at time t is formulated as (3) where T is a fixed total time period before t and always divisible by Δt. Based on the distribution system, operators of a specific distribution system can decide on the Δt and T.

$$CNAR_t = \sum_{j=1}^{\frac{T}{\Delta t}} \frac{T}{j\Delta t} NAR_{t-j\Delta t} \tag{3}$$

Then, IoT Trustability Score (ITS) for time t is calculated using (4) where $CNAR$s part ensures the stability of the score by gradually changing it for actual anomalies in the data points over certain reporting Δt periods rather than sudden changes at time t due to some short events which are not harmful to the IoT devices.

$$ITS_t = w_t \times NAR_t + w_{t-} \times \frac{CNAR_t}{CNAR_{max}} \tag{4}$$

where,

$$w_t \geq w_{t-} \quad \& \quad w_t + w_{t-} = 1 \tag{5}$$

Here, $CNAR_{max}$ is calculated using (3) with maximum NAR value which is $NAR = 1$ for whole T time period. Operator of the distribution system will choose w_t and w_{t-} based on the system satisfying (5) so that ITS_t depends more on current time NAR while retaining immediate past behaviours of IoTs. Finally to get the overall ITS of any primary node with IoTs, we average the ITS_t of all the clients of that primary node to calculate ITS as,

$$ITS = \frac{\sum_{i=1}^{M} ITS_{t,i}}{M} \tag{6}$$

where M is the total clients or buildings/houses of that primary node.

IV. Primary Level Node Resiliency (PNR) Metric Formulation

A. *Factors Influencing Resiliency*

Modeling and analysis of cyber-power systems help us determine the factors responsible for the resilient operation of the system. These factors vary along with the configuration. Factors that can be determined directly from the secondary level configuration of each primary node are described below.

1) Available generation: The total amount of generation capacity in the secondary level is considered in this factor. Generation from PV, stored energy from storage, etc., are included here. The total committed amount of power supply by all the participants from the downstream of any primary node is the available generation for that node.

2) Amount of critical load: For any primary node, the total amount of critical load located downstream of that node is considered for this factor.

3) Connectivity redundancy: Graph topology-based physical connectivity is used to determine the connectivity redundancy among all the critical loads presented downstream of any primary node, all the secondary nodes with power supply capacity, and the primary node. This considers all the possible paths through which a critical load can get a power supply for normal operation.

4) Device and communication vulnerabilities in Secondary Network: The common vulnerability scoring system (CVSS) [34] is one of several methods to measure the impact of vulnerabilities in devices known as Common Vulnerabilities and Exposures (CVE). It is an open set of standards used to assess a vulnerability of software and assign a severity along a scale of 0-10 [35]. National Institute of Standards and Technology (NIST) analyzes all identified vulnerabilities and enlists them in NIST's National Vulnerability Database (NVD). At first, all the device and communication vulnerabilities presented in the secondary (DCVS) level of a primary node are identified using the NVD. Then DCVS factor is calculated as,

$$DCVS = \frac{1}{\sum_{s=1}^{N_s} CVSS_s} \tag{7}$$

where N_s is the number of total vulnerabilities presented in the secondary level. In case of the absence of any vulnerability, DCVS will be equal to 1.

5) IoT Trustability Score: ITS determines the IoT devices' trustability presented in any primary node and its downstream. Formulation of ITS is described in III-C.

Table II shows the factors considered for resiliency calculation for each type of distribution system configurations.

TABLE II
FACTORS CONSIDERED FOR RESILIENCY CALCULATION OF EACH TYPE OF CONFIGURATION.

Primary node configuration	Factors
Physical Primary Node	Available generation Amount of critical load Connectivity redundancy
Cyber-power Primary Node without IoTs	Available generation Amount of critical load Connectivity redundancy Device and communication vulnerabilities
Cyber-power Primary Node with IoTs (Type-A, B, C)	Available generation Amount of critical load Connectivity redundancy Device and communication vulnerabilities IoT Device Trustability Score

B. Weight Assignment and Aggregation

Evaluating the impact of factors in the resiliency of cyber-power power systems is a very complex task. This requires expertise decisions from different domains such as power systems, cyber-power systems, and cyber system experts. It may again raise ambiguities and uncertainties in the existing information, which can be handled by fuzzy multiple-criteria decision-making(MCDM). In Fuzzy MCDM models, the linguistic terms or comparisons of different experts are represented by fuzzy numbers [36].

Fuzzy Analytic Hierarchy Process (Fuzzy AHP) is an improvement of a standard AHP [37] method using the fuzzy logic approach. The fuzzy AHP method incorporates the impreciseness of human judgment raised due to the subjective or qualitative nature of the criteria that exact numbers can not represent. Fuzzy AHP [36] controls the uncertainty and vagueness in the decision makers' opinions through fuzzy set theory. In this work, a fuzzy rating aggregation method [38] is integrated with fuzzy AHP to the incorporated decision of multiple experts. Fuzzy set theory can easily navigate and incorporate all the decisions to evaluate the impacts of each factor.

The linguistic preference values introduced by Saaty in [37] are fuzzified using the triangular fuzzy numbers. Table III shows the triangular fuzzy conversion scale along with Saaty's scale.

Let there be K number of experts. Once all the experts uses above scale to provides their fuzzy pairwise comparison ratings $R_k = (l_k, m_k, u_k), k = 1, 2, ..., K$, the aggregated fuzzy ratings can be defined as [38],

$$R = (l, m, u) \tag{8}$$

where,

$$l = \min_k l_k$$

$$m = \frac{1}{K}\sum_{k=1}^{K} m_k$$

$$u = \max_k u_k$$

The aggregated fuzzy pairwise comparison matrix $D = [R_{ij}]$ is constructed using the aggregated ratings. For n number of factors, fuzzy pairwise comparison matrix will be,

$$D = \begin{bmatrix} (1,1,1) & R_{12} & \cdots & R_{1n} \\ R_{21} & (1,1,1) & \cdots & R_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ R_{n1} & R_{n2} & \cdots & (1,1,1) \end{bmatrix}$$

Then, the fuzzy geometric mean value r_i, for each factor i is computed as

$$r_i = (R_{i1} \times R_{i2} \times ... \times R_{in})^{\frac{1}{n}} \tag{9}$$

The fuzzy weight w_i for each factor is calculated as,

$$w_i = r_i \times (r_1 + r_2 + ... + r_n)^{-1} \tag{10}$$

where, $r_i = (l_i, m_i, u_i)$ and $(r_i)^{-1} = (1/u_i, 1/m_i, 1/l_i)$.

Center of Area method is used to defuzzify the fuzzy weights $w_i = (l_i, m_i, u_i)$ as below to get the weight w_i for each factor.

$$w_i = \frac{l_i + m_i + u_i}{3} \tag{11}$$

Finally, normalization is done to get the final weight W_i for each factor as below,

$$W_i = \frac{w_i}{\sum_{i=1}^{n} w_i} \tag{12}$$

When it comes to aggregation, multiplicative approach offers more superior performance than additive approach [40]. Again, the adoption of multiplicative performance measures is preferred in General Systems Performance Theory [41]. Therefore, weighted product model is used to get primary level node resiliency(PNR) for any node as below,

$$PNR = \prod_{i=1}^{n_c} (F_i)^{W_i} \tag{13}$$

where, c, and n_c indicate the category of primary level node, and total number of factors for that c category respectively.

V. Distribution system Resiliency (DSR) Metric Formulation in Presence of IoTs

Distribution system-level resiliency (DSR) will give us the overall resiliency of the system.

A. Factors Influencing Resiliency

DSR calculation involves attributes from the primary voltage level of distribution system.

1) Primary level node Resiliency: Primary level node resiliency(PNR) considers all the attributes considering the secondary level configuration of a primary node. The value of PNR can be calculated following the method described earlier using (13).

TABLE III
LINGUISTIC PREFERENCES WITH SCALE FOR PAIRWISE COMPARISON [37], [39]

Linguistic preferences	Saaty's Scale	Saaty's Reciprocal Scale	Triangular Fuzzy Scale	Triangular Fuzzy Reciprocal Scale
Equally strong	1	1	(1, 1, 1)	(1, 1, 1)
Moderately strong	3	1/3	(2, 3, 4)	(1/4, 1/3, 1/2)
Strong	5	1/5	(4, 5, 6)	(1/6, 1/5, 1/4)
Very strong	7	1/7	(6, 7, 8)	(1/8, 1/7, 1/6)
Extremely strong	9	1/9	(9, 9, 9)	(1/9, 1/9, 1/9)
Intermediate values	2, 4, 6, 8	1/2, 1/4, 1/6, 1/8	(1, 2, 3), (3, 4, 5), (5, 6, 7), (7, 8, 9)	(1/3, 1/2, 1), (1/5, 1/4, 1/3), (1/7, 1/6, 1/5), (1/9, 1/8, 1/7)

2) Available power outflow: Available power outflow (APO) from the primary node is the difference between the available power from a different generation and storage resources, and the total amount of critical load presented downstream of that primary node.

3) Primary node centrality: Primary node centrality (PNC) provides the importance of a primary level node in the whole distribution in terms of connectivity. In this work, the concept of leverage centrality [42] is utilized to identify the criticality of each network node. The degree of a node relative to its neighbors is considered in Leverage centrality. Leverage centrality identifies nodes connected to more nodes than their neighbors. A well-connected node i can pass information to many neighbor nodes. But if those neighbor nodes have a high degree, they do not need to rely much on that node i. Thus, node i ends up with low leverage in the network. Nodes with high leverage centrality control the content and quality of the information received by their neighbors. Although leverage is derived from degree centrality, it is very effective compared to other centralities in determining the importance of any node in a network where network flow can happen in any direction rather than only along the shortest path or in a serial fashion [42]. With modernization, the distribution system has also become this type of network as power flow can happen in any direction. So, to determine the importance of any individual node in the distribution system network, PNC is formulated using the concept leverage centrality as,

$$PNC_i = \frac{d_i}{\sum_{j \in N_i} d_j} \tag{14}$$

where, N, d_i, N_i, and d_j are the total number of nodes, degree of the given node, directly connected neighbors of the node i and the degree of those neighbors, respectively. PNC formulation in (14) also does not increase computational burden as the distribution system becomes larger.

4) Device and communication vulnerabilities in primary network: Once any vulnerability is identified using NVD presented in the primary level of the distribution system, it is assigned to its corresponding primary node based on the source of the vulnerability. In this way, all vulnerabilities presented at the primary level can be assigned to the primary nodes of the distribution system. Then device and communication vulnerabilities of each primary node (DCVP) is calculated as,

$$DCVP = \frac{1}{\sum_{p=1}^{N_p} CVSS_p} \tag{15}$$

where N_p is the number of total vulnerabilities related to that specific primary level node. In case of the absence of any vulnerability, DCVP will be equal to 1.

B. Weight Assignment and Aggregation

The weight distribution for each factor of each primary node considered in DSR calculation determines the contribution of any node to overall system resiliency. In this work, this weight distribution problem is formulized as a Data Envelopment Analysis (DEA) problem where the "weights" in DEA are derived from the data instead of being fixed in advance [43]. Once all the factors for each of the primary level nodes are calculated during normal operation, a game-theoretic DEA [44] based concept is used to determine the weights so that each node will have the best set of weights.

Let $F = (f_{ij}) \in R_+^{m \times n}$ be the factors value matrix, where f_{ij} is value of factor i of primary node j. The node will contribute more to resiliency metric in regard to that factor as higher the value of f_{ij} goes. Now, following the DEA analysis, each node p can choose a set of weights $w^p = (w_1^p, ...w_m^p)$, where, $\sum_{i=1}^{m} w_i^p = 1$. Now the relative contribution(RC) of the node p to the total contribution of all the nodes towards DSR as measured by node k's weight selection can be evaluated as,

$$RC^p = \frac{\sum_{i=1}^{m} w_i^p f_{ip}}{\sum_{i=1}^{m} w_i^p \sum_{j=1}^{n} (f_{ij})} \tag{16}$$

Now, each node wants to maximize this ratio in (16) to have the the best set of weights so that they can contribute to the maximum possible value in DSR. Again, dominance of any specific factor in comparison to other factors in DSR calculation for different distribution systems can vary depending upon the distribution system configuration. So, we have introduced an option to set a minimum threshold of weight w_i^{ex} for each factor depending upon the distribution system configuration by the operators or experts of that system. All of these result into the following program,

$$\max_{w^p} \frac{\sum_{i=1}^{m} w_i^p f_{ip}}{\sum_{i=1}^{m} w_i^p \sum_{j=1}^{n} (f_{ij})} \tag{17}$$

$$s.t. \quad w_i^k \geq w_i^{ex}, \quad \sum_{i=1}^{m} w_i^k = 1$$

where, $w_i^{ex} = [0, 1]$

Once (17) provides the weight vector for each node, a combination of multiplicative and additive methods are used as below to get the DSR.

$$DSR = \sum_{j=1}^{n} \left(\prod_{i=1}^{m} (f_{ij})^{w_i^j} \right) \tag{18}$$

Few primary nodes in the distribution system do not expand into secondary voltage levels and are just connectivity with other nodes. For this type of primary node, PNC and DCVP factors are considered in (17) and (18).

VI. Case Studies and Results

For case studies, we have selected IEEE 123 node test feeder system as our test system. This test feeder has spot loads in 85 nodes. Since this work focuses on the resiliency of the distribution system in the presence of IoTs, we have modified those spot load nodes to include IoTs. We have categorized 50 nodes as cyber-power primary nodes with IoTs, 20 nodes as cyber-power primary nodes without IoTs, and the rest of the nodes as a physical primary nodes as described in II-B. The case studies have also been structured around IoTs. In this study, we have selected $\Delta t = 1$, $T = 12$, $w_t = 0.5$ and $w_{t-} = 0.5$.

A. Validation of Autoencoders with Federated Learning Architecture of ITS

The major components of the ITS formulation are the autoencoder models with federated learning architecture. We created a validation data set for each type of data to validate those models. Since the effect of any adverse event in IoTs on their data point is still a topic of ongoing research, for now, it is safe to flag any abnormal data point as an anomaly for IoTs. We prepared the validation data set by introducing values for data points beyond the normal range for each data type. Then after training and setting up the T_{err}, the local autoencoders block reconstructed those validation data points, and the ITS algorithm block flagged all the data points with abnormal values as ADP from their RE values as expected.

B. IoT Trustability Score

During normal operation, ITS is always 1.0 which can be seen in Fig. 6 till reporting time step, $t = 14$.

For the first case scenario, we have assumed that solar PV of one house from the primary node in Fig. 2 accidentally got disconnected from its smart IoT-based inverter during maintenance of the PV panel at $t = 14$. The maintenance person quickly noticed it and fixed the connection by $t = 16$. Data points generated during that event from the solar PV became corrupted and resulted in a drop in non-anomaly ratio (NAR) from 1 to 0.75 and bounce back to 1 at $t = 16$ as shown by line ”NAR_sse” in Fig. 6. This event can be classified as an unintended non-malicious event. Though ITS of that primary node registered the event and slightly dropped for that event periods as shown by line ”ITS_sse” in Fig. 6 as expected.

For the second case scenario, we have assumed that two houses and the commercial building use smart IoT-based inverters from the same manufacturer for their solar PV and battery, and attackers have discovered vulnerabilities of the inverters of that manufacturer. Once the attackers have gained access to the inverters at $t = 14$, data points of PVs and batteries start to have irregular values due to the malicious activity of those attackers. NAR of one of those houses described by line ”NAR_me” in Fig. 6 shows a significant drop. Since three out of seven users of that primary node are under attack, ITS of that primary node also degrades a lot, as shown by the line ”ITS_me” in Fig. 6. As the attackers keep gaining full access to those inverters, anomalous data points continue, and ITS also remains degraded as expected.

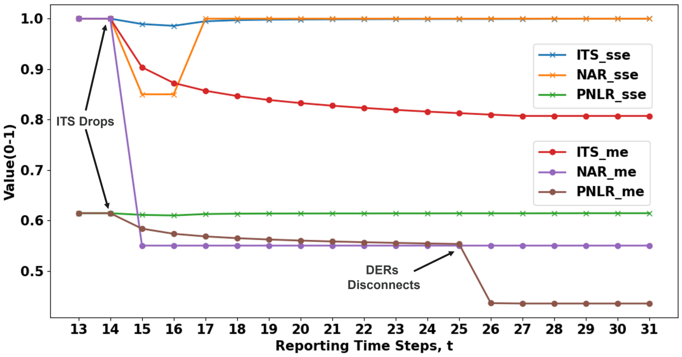

Fig. 6. IoT Trustability Score (ITS) and Primary Node Resiliency (PNR) during case scenarios.

C. Primary level node Resiliency

Now, we will calculate the PNR of the primary node with IoTs shown in Fig. 2. Lets assume, there are two operators or experts and they provide below pairwise comparison matrices for the five factors in the order as described in Table IV,

$$M1 = \begin{bmatrix} 1.0 & 3.0 & 7.0 & 5.0 & 0.333 \\ 0.333 & 1.0 & 2.0 & 7.0 & 0.143 \\ 0.143 & 0.5 & 1.0 & 0.333 & 0.111 \\ 0.2 & 0.143 & 3.0 & 1.0 & 0.111 \\ 3.0 & 7.0 & 9.0 & 9.0 & 1.0 \end{bmatrix} \tag{19}$$

$$M2 = \begin{bmatrix} 1.0 & 2.0 & 5.0 & 6.0 & 0.5 \\ 0.5 & 1.0 & 3.0 & 3.0 & 0.167 \\ 0.2 & 0.333 & 1.0 & 0.333 & 0.125 \\ 0.167 & 0.333 & 3.0 & 1.0 & 0.111 \\ 2.0 & 6.0 & 8.0 & 9.0 & 1.0 \end{bmatrix} \tag{20}$$

Now by following all the steps of fuzzy AHP explained in IV-B, we get the weights shown in Table IV for the factors from these two pairwise comparison matrices.

Now, once all the factors values are determined, we calculate PNR for this cyber-power primary node with IoT using (13) for both case scenarios explained in VI-B and plot in Fig. 6.

PNR for the first case is shown by line ”PNR_sse” in Fig. 6. It does not have a noticeable change in its value as all the factors remain constant except ITS, which also does not change much during the event periods.

For the second case scenario, PNR exhibits significant change as shown by line ”PNR_me” in Fig. 6. At $t = 14$,

TABLE IV
WEIGHTS OF FACTORS FOR A TYPICAL CYBER-POWER PRIMARY NODE WITH IOT

Factors Name	Weight(W_i)
Available generation	0.27
Amount of critical load	0.129
Connectivity redundancy	0.042
Device and communication vulnerabilities	0.055
IoT Trustability Score	0.504

PNR starts dropping as ITS drops. Then, at $t = 25$, the attackers successfully disconnect the solar PVs and batteries associated with those attacked inverters. These disconnections result in the reduction of available generation. Now that another factor loses its value at $t = 25$ along with previously reduced factor ITS, PNR drops again from the next t as shown by line ”PNR_me” in Fig. 6.

D. Distribution system level resiliency

Since primary level node resiliency covers all the secondary voltage areas, which is the most significant part of the distribution system's operation area, it should contribute most to the overall distribution system level resiliency. Therefore, this work chooses the minimum threshold of weights for factors as 0.4, 0.1, 0.1, 0.1, respectively, for PNR, APO, PNC, and $DCVP$. Then, the factors value and their weights are calculated for each reporting time step t and combined to get the distribution system level resiliency as explained in V.

For the first case scenario, we have extended the unintended non-malicious event similar to the event explained earlier to four cyber-power primary nodes with IoTs. One house from those four nodes suffers from an unintentional non-malicious event. As this type of event hardly affects primary level node resiliency of respective primary node, the overall DSR remains the same as shown by line ”DSR_sse” in Fig. 7.

For the second case scenario, we have extended a similar malicious event by considering the presence of smart IoT-based inverters from the same manufacturer in 30 cyber-power primary nodes with IoTs. As attackers attack all of those inverters at $t = 14$, all of 30 nodes experience a significant drop in ITS, reducing PNR of each node as shown earlier. Reduction in PNR of 30 nodes brings down DSR. Then, at $t = 25$, the attackers successfully disconnect all the solar PVs and batteries associated with those attacked inverters. These disconnections result in the reduction of available generation of each of those 30 nodes, which further reduces PNR of each primary node. The available power outflow (APO) factor of each of those 30 nodes also reduces as generation in their secondary level decreases due to these disconnections. Now that another factor APO loses its value at $t = 25$ along with further reduced factor PNR, DSR drops again from the next t as shown by line ”DSR_me” in Fig. 7.

VII. CONCLUSIONS

The introduction of more Internet of Things (IoTs) based Distributed Energy Resources (DERs), loads, and other devices leads to better and efficient operation with flexibility but also brings vulnerabilities. Detailed monitoring of all the resources is becoming critical due to the increasing cyber-attack surface and complexity of the system. This also leads to privacy concerns for users owning IoTs. Federated learning-based monitoring can elevate these problems if data tracking is not possible. Thus, without breaching privacy, the overall resiliency metrics formulation presented in this work can provide situational awareness and critical information to the distribution system operators for a distribution system with IoTs. DSR metrics offer visibility to the edge of the system. With DSR applications running in the distribution system control center, the operators can easily navigate through that information and reach the components impacting resiliency. Then, factors related to those components can be used to quickly investigate the system to analyze the event and take suitable remedial actions. For example, during an event similar to the second case scenario, the operators can utilize the information from DSR, PNR, and ITS to detect malicious activities of the latent threat in the system. Then operators can take timely action such as importing power from external sources to feed the critical loads when PVs and batteries are out of operation due to the attack.

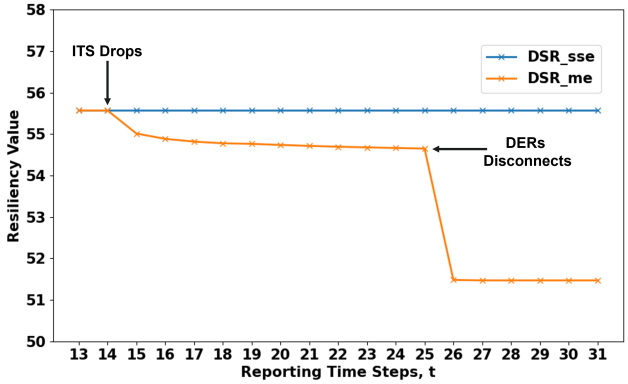

Fig. 7. Distribution System Resiliency during case scenarios on a scale of 0-123 where 123 is the total primary node number of the system.

The proposed metrics are capable to facilitate resiliency based monitoring and operation for any advanced power distribution system. It can easily adapt to any upgrade or change in the distribution system, such as installing new DERs, new smart buildings coming into the grid, etc. Since it calculates the DSR metric according to the total number of primary level nodes in the distribution system, it can be used to make a DSR percentage comparison of different systems. Another benefit of the metrics can also be extended towards offline study for designing the possible resilient distribution system for a given cost. For future work, we can make DSR more robust by developing better models of IoT devices using advanced learning algorithms. Developed metrics can also be utilized to develop an operational reconfiguration algorithm to have the most possible resilient configuration during adverse events.

REFERENCES

[1] M. D. Ilic, L. Xie, U. A. Khan, and J. M. Moura, “Modeling future cyber-physical energy systems,” in *2008 IEEE Power and Energy Society*

General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century. IEEE, 2008, pp. 1–9.

[2] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, pp. 18–28, 2009.

[3] M. D. Ilić, L. Xie, U. A. Khan, and J. M. Moura, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 4, pp. 825–838, 2010.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[5] S. H. Shah and I. Yaqoob, "A survey: Internet of things (iot) technologies, applications and challenges," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*, 2016, pp. 381–385.

[6] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[7] R. Morello, C. De Capua, G. Fulco, and S. C. Mukhopadhyay, "A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and iot in the electric grid of the future," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7828–7837, 2017.

[8] D. Evans, "How the next evolution of the internet is changing everything," 2011.

[9] E. National Academies of Sciences and Medicine, *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press, 2017. [Online]. Available: https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system

[10] N. A. E. R. Corporation, "Severe impact resilience: Considerations and recommendations," 2016.

[11] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1055–1065, mar 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8767980/

[12] Venkataramanan, Venkatesh and Hahn, Adam and Srivastava, Anurag, "CyPhyR: A cyber-physical analysis tool for measuring and enabling resiliency in microgrids," *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, no. 4, pp. 313–321, dec 2019.

[13] A. Uprety and D. B. Rawat, "Reinforcement learning for iot security: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693–8706, 2021.

[14] H. Li, K. Ota, and M. Dong, "Learning iot in edge: Deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[15] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A. R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," *Proceedings - International Conference on Distributed Computing Systems*, vol. 2019-July, pp. 756–767, 2019.

[16] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Enabling ai in future wireless networks: A data life cycle perspective," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 553–595, 2021.

[17] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.

[18] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 806–12 825, 2021.

[19] S. Aheleroff, X. Xu, Y. Lu, M. Aristizabal, J. Pablo Velásquez, B. Joa, and Y. Valencia, "Iot-enabled smart appliances under industry 4.0: A case study," *Advanced Engineering Informatics*, vol. 43, p. 101043, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1474034620300124

[20] Q. Hu and F. Li, "Hardware design of smart home energy management system with dynamic price response," *IEEE Transactions on Smart Grid*, vol. 4, no. 4, pp. 1878–1887, 2013.

[21] D. J. Sebastian, U. Agrawal, A. Tamimi, and A. Hahn, "Der-tee: Secure distributed energy resource operations through trusted execution environments," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6476–6486, 2019.

[22] D. R. Roberto Minerva, Abyi Biru, "Towards a definition of the internet of things (iot)," Available online: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, 2015.

[23] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, 2019. [Online]. Available: https://www.mdpi.com/2411-5134/4/1/22

[24] M. Yun and B. Yuxin, "Research on the architecture and key technology of internet of things (iot) applied on smart grid," in *2010 International Conference on Advances in Energy Engineering*, 2010, pp. 69–72.

[25] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart choice for the smart grid: Narrowband internet of things (nb-iot)," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1505–1515, 2018.

[26] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "Gridlab-d: An open-source power systems modeling and simulation environment," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, 2008, pp. 1–5.

[27] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-physical security and resiliency analysis testbed for critical microgrids with ieee 2030.5," in *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020, pp. 1–6.

[28] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 61–68.

[29] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, "Mininet-wifi: Emulating software-defined wireless networks," in *2015 11th International Conference on Network and Service Management (CNSM)*, 2015, pp. 384–389.

[30] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[31] A. Ahmed, K. S. Sajan, A. Srivastava, and Y. Wu, "Anomaly detection, localization and classification using drifting synchrophasor data streams," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3570–3580, 2021.

[32] T. Luo and S. G. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in wsn for iot," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

[33] F. Chollet *et al.* (2015) Keras. [Online]. Available: https://github.com/fchollet/keras

[34] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[35] "NVD - Vulnerability Metrics." [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

[36] J. J. Buckley, "Fuzzy hierarchical analysis," *Fuzzy sets and systems*, vol. 17, no. 3, pp. 233–247, 1985.

[37] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European journal of operational research*, vol. 48, no. 1, pp. 9–26, 1990.

[38] C.-T. Chen, C.-T. Lin, and S.-F. Huang, "A fuzzy approach for supplier evaluation and selection in supply chain management," *International journal of production economics*, vol. 102, no. 2, pp. 289–301, 2006.

[39] D. Kannan, R. Khodaverdi, L. Olfat, A. Jafarian, and A. Diabat, "Integrated fuzzy multi criteria decision making method and multi-objective programming approach for supplier selection and order allocation in a green supply chain," *Journal of Cleaner production*, vol. 47, pp. 355–367, 2013.

[40] C. Tofallis, "Add or Multiply? A Tutorial on Ranking and Choosing with Multiple Criteria," *INFORMS Transactions on Education*, vol. 14, no. 3, pp. 109–119, May 2014. [Online]. Available: http://pubsonline.informs.org/doi/abs/10.1287/ited.2013.0124

[41] G. V. Kondraske, "General systems performance theory and its application to understanding complex system performance," *Information Knowledge Systems Management*, vol. 10, no. 1-4, pp. 235–259, 2011. [Online]. Available: https://content.iospress.com/articles/information-knowledge-systems-management/iks00195

[42] K. E. Joyce, P. J. Laurienti, J. H. Burdette, and S. Hayasaka, "A New Measure of Centrality for Brain Networks," *PLoS ONE*, vol. 5, no. 8, p. e12200, Aug. 2010.

[43] A. Charnes, W. W. Cooper, and E. Rhodes, "Measuring the efficiency of decision making units," *European journal of operational research*, vol. 2, no. 6, pp. 429–444, 1978.

[44] K. Nakabayashi and K. Tone, "Egoist's dilemma: a DEA game," *Omega*, vol. 34, no. 2, pp. 135–148, Apr. 2006.