Privacy-Preserving Information Security for the Energy Grid of Things

Mohammed Alsaid[1][a], Nirupama Bulusu[1], Abdullah Bargouti[2], N. Sonali Fernando[2], John M. Acken[2], Tylor Slay[2], and Robert B. Bass[2][b]

[1]*Maseeh College of Engineering and Computer Science, Department of Computer Science, Portland State University, Portland, USA*

[2]*Maseeh College of Engineering and Computer Science, Department of Electrical & Computer Engineering, Portland State University, Portland, USA*

{*alsaid, nbulusu, abdb2, narmada, acken, tslay, robert.bass*}*@pdx.edu*

Keywords: *Smart Grid, Security, Privacy.*

Abstract: Smart grid infrastructure relies on information exchange between multiple actors in order to ensure system reliability. These actors include but are not limited to smart loads, grid control, and energy management technologies. As information exchange between these actors is susceptible to cyber-attacks, security and privacy issues are indispensable to ensure a reliable and stable grid. This position paper proposes a privacy-preserving, trust-augmented secure scheme for a smart grid implementation.

1 INTRODUCTION

The concept of a smart electric power grid can be defined as a network of grid-interactive generators, storage systems, and loads that exchange information to ensure system reliability, resource adequacy, and economical provision of electrical power. Unlike the traditional electrical grids, where power is uni-directional, power within a smart grid is instead bi-directional. Grid-interactive devices can be managed efficiently to source, store, and consume power as both demand and supply fluctuate (Adham et al., 2022). Moreover, a smart grid relies heavily on automated digital interactions between its components. This makes it an attractive target for all types of adversaries. Thus, it is of the utmost importance to address the security of information exchanged between system actors and ensure customer information privacy.

For critical infrastructure like electric power systems, a cyber-attack could be catastrophic. Knowing that information exchange within a smart grid is susceptible to cyber-attacks, it is imperative that system designers address security and privacy problems to ensure reliable and stable power systems. Multiple industry standards have been developed for managing information exchange within power systems, and several include security features, such as IEEE 2030.5 and OpenADR (Obert et al., 2019; Herberg et al., 2014; Obi et al., 2020).

Following industry standards with little understanding of the system to be developed may produce a complex system with undetected vulnerabilities (Myagmar et al., 2005). One systematic approach to finding vulnerabilities of a system is through creating a threat model for the system at hand. The creation of a threat model is an iterative process. It requires one to repeatedly revisit the design and reexamine the interactions between the system components, identify the assets, and identify the threats. Implementing a threat model requires identifying security vulnerabilities and possible mitigation strategies, which can serve as the foundation of the system's security.

Identifying assets in threat modeling entails listing all resources to protect, either abstract or concrete. Identifying threats requires inspecting the possible goals of the assumed adversaries. There are several methods to identify common threats, such as relying on mnemonics like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) or using frameworks that utilize different metrics like Common Vulnerability Scoring System (CVSS) and Security Cards (Bodeau et al., 2018). The process of drafting security requirements necessitates reviewing all the identified

[a] https://orcid.org/0000-0003-0792-5287

[b] https://orcid.org/0000-0002-5644-4634

threats. For every threat, the goal is to manage its associated risk by assessing whether to mitigate it or accept it based on the threat's severity and the likelihood of its occurrence.

To explore how this position paper addresses security threats and privacy-preserving features, we structured the manuscript as follows: A survey of related work is presented in section 2. A brief overview of Energy Grid of Things (EGoT) is presented in section 3. Adversary and thread models are considered in section 4. Privacy aspects of the EGoT are discussed in section 5. Security within the EGoT is discussed in section 6, and trust modeling for unpredictable attack scenarios is presented in section 7. This is followed by the conclusion in section 8.

Acronyms

ACL Access Control List

CDTA Central Distributed Trust Aggregator

COSEM Companion Specification for Energy Metering

CVSS Common Vulnerability Scoring System

DCM Distributed Control Module

DER Distributed Energy Resources

DLMS Device Language Message Specification

DoS Denial of Service

DTM Distributed Trust Model

DTMC Distributed Trust Model Client

EGoT Energy Grid of Things

ESI Energy Services Interface

FDI False Data Injection

GO Grid Operator

GSP Grid Service Provider

HE Homomorphic Encryption

LoPA Low-overhead Privacy Aggregation

MVoT Metric Vector of Trust

SPC Service-Provisioning Customer

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

2 Related Work

There exists extensive prior work within the security community related to smart grid security over the last decade. Such work is the foundation of many new research trajectories, including ours. This section of the paper presents closely-related work to our implementation. Moreover, we briefly discuss how our work has been influenced by and differs from the examined earlier work.

Salinas, Sergio, and Li propose two different algorithms to detect energy theft in smart grids (Salinas and Li, 2016). The authors provide a State Estimation with Kalman filter (SEK) algorithm that uses Kalman filter for theft detection. However, SEK violates users' privacy by using their characteristic load profiles (current and voltage). The authors also propose a Privacy-Preserving Bias Estimation (PPBE) algorithm, which preserves users' privacy through loosely decoupling filters. Finally, the authors show that PPBE converges faster than SEK regarding true-value bias estimation. Our work does not address energy theft detection. Moreover, load profiles in EGoT are kept local instead of being shared with external entities.

Defend and Kursawe present a privacy-preserving implementation of the smart grid concept (Defend and Kursawe, 2013). Their implementation makes use of an Low-overhead Privacy Aggregation approach. The implementation uses data aggregation and Homomorphic Encryption (HE) in smart meters to preserve the privacy of customers. It also provides an assessment of the scalability and integration of the approach with standards like Device Language Message Specification and Companion Specification for Energy Metering. Finally, the authors show that their system poses little overhead in CPU usage and the time needed to perform encryption operations.

Wei-jing et al. present a similar approach, which uses Paillier and El-Gamal signature algorithms to protect user privacy (Wei-jing et al., 2019). The authors show that their proposed method also protects users' identities and power consumption. In the EGoT smart grid implementation, we make use of data aggregation as a means of preserving privacy. We address this more in the privacy section of this paper. However, we are not using HE to protect privacy. Instead, we use randomized energy requests to obfuscate the user's behavioral patterns. Nonetheless, HE shows promise as an additional layer of privacy protection that could complement our work in the future.

Deng, Zhuang, and Liang proposed a model for a practical False Data Injection (FDI) attack against state estimation in distribution systems (Deng et al.,

2019). The authors show that power flow in distribution systems can expose information that helps attackers estimate the system state. Furthermore, an IEEE test feeder was used to simulate the FDI attack, and the results showed that such an attack is plausible to compromise the system. Contrary to the proposed smart grid implementation, the addition of grid equipment requires out-of-band registration, which is outside the scope of EGoT scheme. Further, participating actors in EGoT must be authenticated and authorized by Grid Service Provider servers before processing received information. Finally, detective measures are to be installed to validate sensors readings' trustworthiness as another line of defense against such an attack.

3 Energy Grid of Things

Our implementation of the smart grid is referred to as an EGoT. Three main layers make up the EGoT. The power layer concerns the distribution of energy to households. The network layer governs how Distributed Energy Resources (DER) within the EGoT exchange information. And, the trust layer defines the aggregate trust within the system. When a DER is dispatched, the states of all three layers are affected: through the network layer, the DER informs the aggregator of its availability and its energy and power requirements; the trust layer monitors the information exchange between actors and adjusts the trust scores of those involved accordingly; and, within the power layer, requested energy exchange occurs between the Grid Operator and the DER.

The EGoT is an implementation of the smart grid concept. It relies on the IEEE 2030.5 protocol, known as the Smart Energy Profile 2.0 (anon., 2018a) to communicate energy and power information, pricing-related information, and scheduling to arrange resources for large-scale aggregated dispatch of DERs. DERs are grid-enabled, customer-owned generation, storage, and load assets. These resources are located behind customers' meters and are not traditionally directly managed by utilities. DERs can be dispatched to consume energy, like water heaters (Marnell et al., 2020), or they can be configured to inject energy back into the grid when it is needed, like inverter-based systems (Hossain and Ali, 2013; Hoke et al., 2018). Households that host DERs are referred to as Service-Provisioning Customers (SPCs).

An EGoT system allows a Grid Service Provider (GSP) to provide grid services[1] to a Grid Operator (GO) through the coordinated dispatch of large numbers of DERs. GOs use grid services to maintain bulk power system frequency and voltages to ensure reliable energy transfer, which can be negatively impacted by changes in load or variations in renewable energy generation (Carvalho et al., 2008; Zarina et al., 2012).

The EGoT system follows a server-client architecture, wherein the server is hosted by a GSP and the Distributed Control Modules (DCMs) are the clients. SPCs subscribe their DERs to GSP programs, which can be dispatched to provide grid services based on their availability, dispatch characteristics, and topological location. The GSP server provides a means for a GO to requisition grid services through large-scale aggregation and coordinated dispatch of DERs.

An Energy Services Interface (ESI) serves as a demarcation boundary between GSP and SPCs (Lee et al., 2013). It defines a set of rules regarding the information exchange between system actors on either side of the boundary (Slay and Bass, 2021). These rules define a bi-directional, service-oriented, logical interface that supports secure, trustworthy information exchange between the GSP and the SPCs' DERs (Widergren et al., 2019). The ESI is bidirectional in that devices on the SPC-side can send requests to GSP servers and receive responses.

Due to the variability of DER manufacturers and the heterogeneity of the protocols they obey, there must be mechanisms for ensuring interoperability. Interoperability in an EGoT system is accomplished through software and hardware support. DCMs within the EGoT are tasked with expanding DER functionalities such as the support of IEEE 2030.5 messaging, scheduling, and network communication. Therefore, DCMs are the realization of hardware and software support for interoperability.

The Distributed Trust Model (DTM) System is an augmentation to existing security for the EGoT system. The DTM System monitors information exchange between various energy grid actors and provides measures of trustworthiness among the actors (Fernando et al., 2021). The DTM System consists of two parts: a Central Distributed Trust Aggregator (CDTA), located at the GSP, and numerous DTM clients, located along with the DCMs at each of the SPCs, as depicted in Figure 1.

The DTM system expresses trustworthiness using a Metric Vector of Trust (MVoT). Each DTM within the SPC maintains an MVoT for each of the actors that communicate with its DCM host. Consider DTMC-a on the right side of Figure 1; this DTM is paired with a DCM, which communicates with DER-a and

[1]U.S. Federal Energy Regulatory Commission, "Guide to Market Oversight Glossary", March 15, 2016

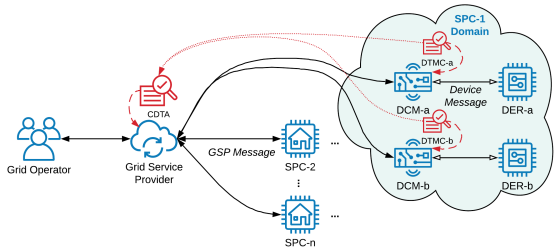

Figure 1: Shown are the communication links between the EGoT System actors (blue), the DTM System actors (red). The DTM System monitors information exchange between the EGoT System actors.

the GSP. So, the DTM maintains an MVoT for each of these actors: DCM-a, DER-a and the GSP. The MVoT includes 17 parameters. The DTM system evaluates the participating actors and quantifies parameters such as trust, distrust, and certainty using the MVoT.

The DTM at the SPC is responsible for evaluating and classifying messages to and from the DCM and to populate the MVoT parameters based on information exchange between the DCM, its DER, and the GSP. The DTM maintains an MVoT for each of these actors. The CDTA is responsible for aggregating all Distributed Trust Model Client (DTMC) MVoTs, comparing the various MVoT parameters with threshold values, and sending messages/alerts to the appropriate authorities. Section 7 covers the architecture of the DTM system in detail.

4 Adversary and Threat Model

The assumed adversary categories in EGoT include tech-savvy users and nation-backed adversaries. The class of tech-savvy users describes a group of users who may have malicious intentions with limited resources to launch scathing attacks. Tech-savvy user skills might enable exposure of the system protocol to identify and exploit undiscovered vulnerabilities. The motivation for the tech-savvy users might be to conduct further reconnaissance of a specific target or game the system for financial incentives without revealing DERs identities to the GSPs. This can be done with falsified DER identities.

Nations-backed adversaries already have the requisite expertise and resources to initiate destructive attacks to the grid (Liang et al., 2017; Langner, 2011). Unlike tech-savvy users, nation-backed adversaries have more resources, expertise, and motives to inflict real damage on the grid. State-level adversaries' are motivated to cause financial losses, blackouts, or other political damage. The complexity of attacks they can instigate is much higher relative to the other two categories.

Threats for the smart grid might be malicious and could be caused by adversaries, unfriendly entities, or due to errors such as equipment failure and administrative errors (Li et al., 2019). The latter type of threat is out of the scope of this analysis. The following diagram depicts a network model of EGoT to highlight interactions between actors.

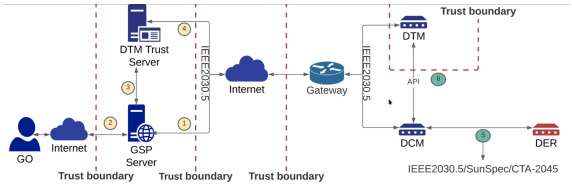

Figure 2: Demonstrates the communication between the different components of EGoT. The figure shows the interaction between the GO (left), GSP (middle), and a single SPC (right).

As conveyed in Figure 2, the red dotted lines indicate trust boundaries with various trust levels. Further, circled numbers indicate a data exchange point between actors. For brevity, the data flow within the actors' components is out of the scope of the analysis. Similarly, the diagram excludes data flow within the GOs site as well.

Since the EGoT relies on the voluntary participation of DERs to fulfill grid services, DERs are considered to be assets. Furthermore, GSPs are the primary actors responsible for managing grid services through the dispatch of DERs. Therefore, any malicious attempts to target the availability of DERs or GSPs pose a threat to the system's stability. For example, communication between the GSP and SPCs is routed through the internet shown in Figure 2. A Denial of Service (DoS) attack targeted at either party may prove disastrous given that adversaries are aware of the grid state and those grid emergencies require a timely response (Kalluri et al., 2016).

Data consistency throughout the components of the grid is also an abstract asset. Due to a FDI attack or other reasons, inconsistent data could cause incorrect grid services to be carried out, which may lead to an unstable electrical system (Deng et al., 2019). Furthermore, the messages between GOs and GSPs are routed through the internet, making them vulnerable to cybersecurity threats (Pliatsios et al., 2020). The corresponding point of data flow, number 2 in Figure 2, expresses a summary of grid conditions sent by the GSP to the GO, and the GO sends its needs to the GSP. Any false communication could lead to incorrect grid services being carried out. For instance, spoofing the GO and instructing GSPs to

continue normal operations during grid emergencies would be catastrophic (Teixeira et al., 2014; Isozaki et al., 2016). Likewise, updating the GOs with erroneous grid states may lead the GO to take misguided decisions (Deng et al., 2017).

5 Privacy

The principle of least privilege declares that entities should receive the least amount of access required to perform their functions (Saltzer and Schroeder, 1975). Knowledge of grid parameters and states is undoubtedly fundamental to GSP operation. Nonetheless, knowledge of specific DER device information is not crucial to GSP decisions for achieving operational objectives. For instance, knowing the energy consumption of a DER is unquestionably essential to deliver energy to the DER; however, knowing the type of the device is a piece of supplemental, unnecessary information to GSPs operation. Essentially, the ESI goals are to keep DER-related information confined within the SPC 's personal domain and to minimize or obfuscate information that is needed for aggregate dispatch.

The privacy preservation goals call for ground rules that govern actors' interactions. As such, the purpose of the ESI is the enactment of rules that promote privacy within the EGoT (anon., 2018b). For instance, the ESI specifies that GSPs are to engage with SPCs on an opt-in basis; this allows SPCs to decommit from a resource service at any time without penalty. Therefore, SPCs initiates all communication with the GSP.

The stability of the grid is partially dependent on the GSP 's control over resources during grid emergencies (anon., 2014). The ESI rules provide accommodation for DER control by the GSP. However, to conform with the ESI rules, the SPC must be the one to instigate and grant permission for the action. Additionally, the control must be temporary and not for a non-deterministic period.

Data aggregation serves as an approach to preserve privacy. A drawback of data aggregation in a real-world setting is the need for enough parties to participate for this measure to be effective and practical. Another helpful technique is the randomization of energy dispatch, which would also help preserve privacy.

Localization of private information is the primary approach used in this research. This preserves privacy by following the logic that information that is not shared is hard to infer. However, this does not always work as utility companies need access to information that is partly sensitive. For example, estimating the energy consumption of households could be beneficial for price estimation. Yet, this should not require consumers to share their daily energy consumption patterns. The previously mentioned example could be expanded to an entire local area as opposed to an individual household. This is done in the EGoT system through data aggregation by the GSP. That is, private data regarding the user is kept local to the SPC as much as possible. When there is a need to share sensitive information, randomization is used before consumers request energy. Moreover, GSPs aggregate the energy needs of an entire area such that utilities are able to operate on the data in a useful manner without infringing upon the customers' privacy.

6 Securing Information Exchange

Security for the EGoT is divided into two categories: preventative measures and detective measures. The preventive measures include encryption and authentication, as specified in IEEE 2030.5, while the DTM System provides the detective measures. Both categories complement each other to mitigate the threats mentioned in 4. For example, FDI behavior can be observed through unexpected signatures monitored by the DTM system via abnormal MVoT values and inconsistencies of monitored messages. Attacks that rely on flooding traffic are also flagged as abnormal for violating the regular message frequency in MVoT values. The following section expands on the detective measures provided by the DTM System.

IEEE 2030.5 protocol stack includes HTTPS with TLS 1.2. This provides encryption and authentication to secure messages over the internet. Certificate fingerprints, which are derived from hashing the device certificate, are required during deployment and ongoing operations with GSP servers. This reduces the system's susceptibility to spoofing attacks. Furthermore, Access Control Lists (ACLs) are maintained by the GSP to enforce authorization policies. Device permissions are verified before taking action when a request is received, which helps guard against attempts to escalate privileges.

7 Trust Modeling for Unpredictable Attack Scenarios

The sole responsibility of the DTM System is to monitor and alert authorities of any abnormal activities. It is an augmented security solution that enhances existing security without any interference. There are many

advantages of having a DTM due to its ability to fit into many types of communication networks and its customizability to address trust based on the network location, network type, and the type of information exchange between network nodes. Abdul-Rahman and Halles mentioned how the existing security covers only the privacy, authenticity, and access control methods (Abdul-Rahman and Hailes, 1997). Privacy protects information exchange using techniques such as cryptography. Authentication is achieved using a digital signature to ensure authorized parties send and receive messages. Access control ensures that only the intended party accesses the data. In the IEEE 2030.5 protocol, those listed solutions are addressed and accommodated. However, there is no way to ensure if the sender of a message is a malicious party since there is no existing method to verify if an authentic node sent the message. Hence, security needs a fourth element: "trustworthiness."

There are many features a DTM can have. Fernando et al. presented descriptions of many trust model characteristics and DTM design considerations of how the DTM can be present in digital communication networks such as peer-to-peer, hierarchical, or centralized (Fernando et al., 2021). They also provided descriptions of trust model components such as storage solutions, trust equations, etc.

A primary goal of designing a DTM system for the power grid is to ensure its design is fit for the digital communication network architecture. Another is to ensure abnormalities of messages are captured correctly. Also, trust is calculated, and using historical data or real data to calculate trust is also essential. A dynamic DTM design can also have a trust vector where a set of variables can independently identify a specific abnormality as a sign of attack. For example, a trust vector can use a variable to evaluate the changes in the frequency of communication, where communication increase is a sign of a DoS attack.

A vital feature of the DTM System is its ability to monitor digital communication on a network without interference. One part of the DTM System has predetermined knowledge of actor behavior, the type of messages exchanged, and the order they need to be sent/received. With this knowledge, the DTM System can compare the ongoing messages exchanged between actors and their behavior and identify abnormalities. The DTM System is also able to classify messages to be indeterminate. The flexibility of the DTM System ensures it does not make rigid classifications of indeterminate activities yet still flags them for authority figures to evaluate.

One scenario of a DTM system is shown in Figure 3 (Fernando et al., 2021). As illustrated in this Figure, the DTM on the client side receives a raw input message from an actor. The input classifier at the DTM client processes the raw data and classifies the message to be *expected*, *unexpected*, *indeterminate*, *disconnect*, or *none*, along with the message sent time and transit time, and information about the sender of the message.

A message is classified as *expected* if the message is in order and all the required message content is present for a specific transaction. A message is classified as *unexpected* if it is out of order or contains values out of range or message fields containing different data types than expected. An input message is classified as *indeterminate* if the DTM is unable to classify the message precisely. A message is classified as *disconnect* if a DER device does not respond in a timely fashion. An input message is classified as *none* if any of the message contents are incorrect or missing. The classified message is processed in the trust equation evaluation block following classification. The trust equation evaluation block takes in the content generated by the input classifier block and the trust vector, MVoT.

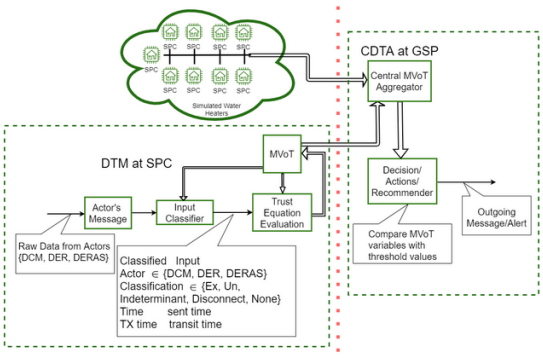

Figure 3: This figure shows the overall connection of the DTM system. Left of the red dotted lines are components of the DTM-Client at the SPC. Right of the red dotted lines are components of the CDTA at the GSP.

The trust vector can contain variables such as:

- Trust Score
- Distrust Score
- Certainty
- Recent up time

where each variable of the MVoT can detect a specific abnormality, Trust Score quantifies an actor's overall trust, while Distrust Score quantifies the actor's overall distrust. Certainty represents how confident the DTM is of the actor who sent the message. The DTM MVoT can be expanded to add n number of variables to detect additional abnormalities.

Each variable has a corresponding equation that the trust model uses to calculate a value for that actor for each specific message. The DTM client updates the new MVoT variables to the CDTA. The responsibility of the CDTA is to compare against those set of thresholds for each alert message and send out alerts to the right authoritative figures/actors if the count exceeds the threshold value.

8 Conclusion

Plans to automate the electrical power grid give way for adversaries to conduct malicious activities. Communication between smart grid components is susceptible to cyber-attacks. In addition, communication patterns could describe customers' behavior, violating their privacy. A privacy-preserving scheme for the smart grid was presented in this position paper. We conducted a threat analysis to assess the security standing of the design—finally, we discussed how privacy is preserved through trust-augmented security measures under the proposed strategy.

REFERENCES

Abdul-Rahman, A. and Hailes, S. (1997). A distributed trust model. In *Proc. of Workshop on New Security Paradigms*, pages 48–60, Langsdale, Cumbira, UK.

Adham, M., Obi, M., and Bass., R. (2022). A field test of direct load control of water heaters and its implications for consumers. In *IEEE PES GM*. submitted for publication.

anon. (2014). Essential Reliability Services Task Force: A Concept Paper on Essential Reliability Services that Characterizes Bulk Power System Reliability. Technical report, North American Electric Reliability Corporation.

anon. (2018a). IEEE standard for smart energy profile application protocol. *IEEE Std 2030.5-2018*.

anon. (2018b). Interoperability strategic vision: A GMLC white paper. PNNL-27320. Technical report, Pacific Northwest National Laboratory.

Bodeau, D. J., McCollum, C. D., and Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. Technical report, Homeland Security Systems Engineering & Development Institute.

Carvalho, P., Correia, P., and Ferreira, L. (2008). Distributed reactive power generation control for voltage rise mitigation in distribution networks. *IEEE Trans. on Power Sys.*, 23(2):766–772.

Defend, B. and Kursawe, K. (2013). Implementation of privacy-friendly aggregation for the smart grid. In *ACM Workshop on Smart Energy Grid Security*, page 65–74, New York, NY, USA.

Deng, R., Xiao, G., Lu, R., Liang, H., and Vasilakos, A. (2017). False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Trans. on Industrial Informatics*, 13(2):411–423.

Deng, R., Zhuang, P., and Liang, H. (2019). False data injection attacks against state estimation in power distribution systems. *IEEE Trans. on Smart Grid*, 10(3):2871–2881.

Fernando, N., Acken, J., and Bass, R. (2021). Developing a distributed trust model for distributed energy resources. In *IEEE Conf. on Tech. for Sustainability*.

Herberg, U., Mashima, D., Jetcheva, J. G., and Mirzazad-Barijough, S. (2014). OpenADR 2.0 deployment architectures: Options and implications. In *IEEE Int. Conf. on Smart Grid Comm.*, pages 782–787.

Hoke, A., Giraldez, J., Palmintier, B., Ifuku, E., Asano, M., Ueda, R., and Symko-Davies, M. (2018). Setting the smart solar standard: Collaborations between Hawaiian Electric and the National Renewable Energy Laboratory. *IEEE Power & Energy Mag.*, 16(6):18–29.

Hossain, M. and Ali, M. (2013). Small scale energy storage for power fluctuation minimization with spatially diverged PV plants. *Proc. IEEE Southeastcon*.

Isozaki, Y., Yoshizawa, S., F., Y., Ishii, H., Ono, I., Onoda, T., and Hayashi, Y. (2016). Detection of cyber attacks against voltage control in distribution power grids with PVs. *IEEE Trans. on Smart Grid*, 7(4):1824–1835.

Kalluri, R., Mahendra, L., Kumar, R., and Prasad, G. (2016). Simulation and impact analysis of denial-of-service attacks on power SCADA. In *National Power Sys. Conf.*

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51.

Lee, E., Gadh, R., and Gerla, M. (2013). Energy service interface: Accessing to customer energy resources for smart grid interoperation. *IEEE J. on Selected Areas in Comm.*, 31(7):1195–1204.

Li, F., Yan, X., Xie, Y., Sang, Z., and Yuan, X. (2019). A review of cyber-attack methods in cyber-physical power system. In *IEEE 8th Int. Conf. on Adv. Power Sys. Automation & Protection*, pages 1335–1339.

Liang, G., Weller, S., Zhao, J., Luo, F., and Dong, Z. (2017). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. on Power Sys.*, 32(4):3317–3318.

Marnell, K., Eustis, C., and Bass, R. (2020). Resource study of large-scale electric water heater aggregation. *IEEE Open Access J. of Power & Energy*, 7:82–90.

Myagmar, S., Lee, A., and Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *Proc. of the IEEE Symp. on Requ. Eng. for Inf. Security*.

Obert, J., Cordeiro, P., Johnson, J., Lum, G., Tansy, T., Pala, M., and Ih, R. (2019). Recommendations for trust and encryption in DER interoperability standards. Technical report, Sandia National Laboratories, SAND2019–1490.

Obi, M., Slay, T., and Bass, R. (2020). Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards. *Energy Reports*, 6:2358–2369.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., and Sarigiannidis, A. (2020). A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Comm. Surveys & Tutorials*, 22(3):1942–1976.

Salinas, S. A. and Li, P. (2016). Privacy-preserving energy theft detection in microgrids: A state estimation approach. *IEEE Trans. on Power Sys.*, 31(2):883–894.

Saltzer, J. and Schroeder, M. (1975). The protection of information in computer systems. *Proc. of the IEEE*, 63(9):1278–1308.

Slay, T. and Bass, R. (2021). An energy service interface for distributed energy resources. In *IEEE Conf. on Tech. for Sustainability*.

Teixeira, A., Dán, G., Sandberg, H., Berthier, R., Bobba, R., and Valdes, A. (2014). Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures. In *American Control Conf.*, pages 4372–4378.

Wei-jing, Z., He-chun, Z., Shi-ying, Y., and Tong, L. (2019). A homomorphic encryption-based privacy preserving data aggregation scheme for smart grid. In *15th Int. Conf. on Comp. Intelligence & Security*, pages 315–319.

Widergren, S., Melton, R., Khandekar, A., Nordman, B., and Knight, M. (2019). The plug-and-play electricity era: Interoperability to integrate anything, anywhere, anytime. *IEEE Power & Energy Mag.*, 17(5):47–58.

Zarina, P., Mishra, S., and Sekhar, P. (2012). Deriving inertial response from a non-inertial PV system for frequency regulation. *IEEE Int. Conf. on Power Electr., Drives and Energy Sys.*, pages 1245–1249.