5-2024

Trust Model Measurements for the Energy Grid of Things

N. Sonali Fernando
Portland State University, narmada@pdx.edu

John M. Acken
Portland State University, john.acken@pdx.edu

Robert Bass
Portland State University, rbass2@pdx.edu

Citation Details

N. S. Fernando, J. M. Acken and R. B. Bass, "Trust Model Measurements for the Energy Grid of Things," 2024 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Anaheim, CA, USA, 2024

Trust Model Measurements for the Energy Grid of Things

N. Sonali Fernando
ECE Department
Portland State University
Portland, Oregon, USA
narmada@pdx.edu

John M. Acken, Ph.D.
ECE Department
Portland State University
Portland, Oregon, USA
acken@pdx.edu

Robert B. Bass, Ph.D.
ECE Department
Portland State University
Portland, Oregon, USA
robert.bass@pdx.edu

***Abstract*—Information security is essential for the reliable operation of an Energy Grid of Things (EGoT). In addition to basic information security protocols as defined by published standards, there is a need for a monitoring function that measures the trustworthiness of the various actors participating in an EGoT. We describe in this paper the implementation and evaluation of a Distributed Trust Model that was developed specifically for monitoring communication within an EGoT. We then show how the model parameters are set using statistical measures for hypothesis testing.**

***Index Terms*—Energy Grid of Things, EGoT, Smart Grid Security, Trust Model, DER, Distributed Energy Resources**

I. Introduction

An Energy Grid of Things (EGoT) is a two-way communication system between energy consumers and energy service providers [1]. This emerging field has significant growth potential, although it is susceptible to many security vulnerabilities. Consumer participation in an EGoT is hindered by privacy and security concerns [2]. If these concerns are addressed properly, then the general public would be more inclined to convert their traditional consumer products to Distributed Energy Resources (DER) [3] [4].

To participate in EGoT grid services, the consumer follows the registration process defined by a Grid Operator (GO), such as an electric utility. The consumer's DER then becomes a registered grid participant for an aggregator, a Grid Service Provider (GSP), which accommodates grid service requests from DERs. The registration process set by the GO ensures that the participants in the grid are known to be authorized as long as they abide by the standard protocol [5]. The security of grid participants is compromised if an intruder gains access to their information or controls their interaction with the grid. Therefore, it is the responsibility of the GSP to ensure that grid participants' information is not accessible to outsiders and to detect indications of such behavior as soon as possible.

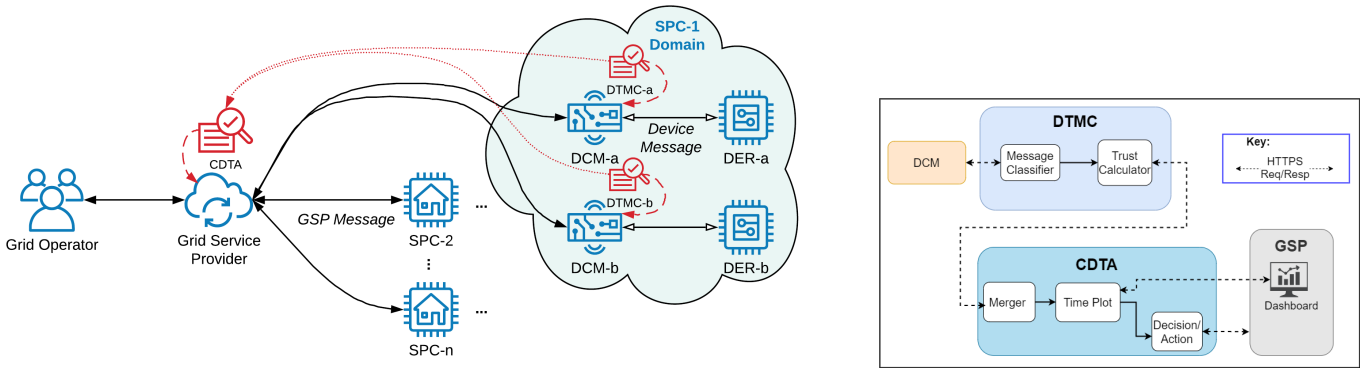
This paper references the IEEE 2030.5 Smart Energy Profile 2.0 (SEP) protocol as the standard that sets security and communication requirements between the GSP and DERs. The security measures for information exchange between the GSP and DERs are specified by the SEP. This manuscript describes an additional layer of security that augments the security implemented by the SEP, the Distributed Trust Model (DTM).

This work was performed under US DOE award DE-OE0000922.

The SEP specifies the following security measurements: Hypertext Transfer Protocol Secure (HTTPS), which is Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) 1.2; Access Control Lists (ACLs); and, registration lists for authorization. TLS uses mutual authentication when establishing communication between the server and the client [6]. TLS has multiple security measures of encryption, message authentication, and data integrity. For encryption, TLS uses Advanced Encryption Standard Cipher Block Chaining - Message Authentication Code (AES-CCM) and requires client-server authentication before establishing a communication channel for message exchange [6]. In addition, it follows the Transmission Control Protocol (TCP) protocol to ensure the encrypted data delivery is reliable and in order between the server and client [6]. Despite the existing security measurements specified by SEP, there is still uncertainty and risk associated with messages and entities in a communication network, and hence there is a need for a DTM system to augment these security measures.

Abdul Rahman and Hailes highlighted a significant security gap in network communication, showing that despite authentication, encryption, and implementation access control, one can not be sure if the correct party provided the encrypted message, even if they provided all the credentials to proceed with a secure communication [7]. Our research adds the idea that even if the correct party does the authentication, there is no way to confirm they are not malicious.

The survey by Kim et al. mentions the current security research and resolutions of a Smart Grid/EGoT are about securing wireless communication between electric vehicles and charging stations [8]. Additionally, EGoT's communication network is vulnerable to Advanced Persistent Threats (APT) attacks, [9]. The DTM can observe for APT when small attacks are conducted in the EGoT communication system. Our research describes a meticulously designed and adaptable Distributed Trust Model system oriented toward conducting assessments of EGoT network communication rather than a preventive solution. The application of a DTM system to an EGoT is a unique security solution. Our DTM system actively monitors EGoT network communication for early detection of



(a) (b)

Fig. 1: DTM-EGoT integration. (a) Integration of DTM into the EGoT system (b) The DTM System described in this paper, designed by the Portland State University's Power Engineering Group.

abnormalities and potential attacks and reports abnormalities to appropriate authorities. In our design, we have a specialized tool, hypothesis testing, that helps authoritative parties who receive the alert messages and set threshold values that meet their preference of when and what alerts to send them. The DTM system analyzes the overall trustworthiness of EGoT network communication, derives diagnostic alert messages that point to potential security threats, and has the flexibility to add more detection features to identify additional attacks.

To address the existing security concerns, the Power Engineering Group at Portland State University implemented a DTM system, Figure 1a and Figure 1b [10] [11]. The goal of the DTM system is to augment the existing security implementation without interference. A unique characteristic of our DTM system is that it is designed specifically for EGoT network communication that follows the SEP messaging scheme. The design is flexible to abide by additional protocols such as OpenADR, Consumer Technology Association (CTA)-2045, DNP3, and SunSpec Modbus, all of which are used by DERs [12].

In this paper, section II presents the architecture of the DTM, followed by section III with the implementation of the DTM Communication. Section IV provides how the DTM communicates abnormalities via the dashboard and messaging scheme. Section V presents scalability testing. Finally, section VI described the hypothesis testing and the procedure for determining threshold values that trigger when to send alerts.

Our DTM system consists of two main components, Distributed Trust Model Clients (DTMCs) and a Central Distributed Trust Aggregator (CDTA). The DTMCs are located at the customers' homes where they check for abnormalities in the communication path between DERs and the GSP. The second component is CDTA, a central unit that collects and analyzes the trust data reported by the DTMCs.

II. DTM Components

DTMCs have two main tasks; first, they classify messages as expected, unexpected, indeterminate, error, or none. The classified messages are then sent to the trust calculator along with the initiating actor's name, message-sent time, and transit time. Then, the DTMCs conduct trust calculation of incoming messages. New trust values are calculated using existing Metric Vector of Trust (MVoT) data and the provided message classification information. Fernando et al. described the MVoT variables and their corresponding equations [13].

Trust Score(TS): Overall trust score for each actor

$$TS = [CExMSG - (\alpha \times CUnMSG)] \times C \tag{1}$$

$CExMSG$ represents the count of messages that are classified as expected. $CUnMSG$ represents the count of unexpected messages.α is a weight that determines the relative influence of $CUnMSG$ relative to $CExMSG$ to be set as the GSP observes the DTM during operation. C is the certainty factor based on the amount of data that has been collected.

Distrust Score(DS): Distrust score for each actor

$$DS = CUnMSG \times C \tag{2}$$

The CDTA aggregates the trust data sent by all DTMCs. It then organizes the data into MVoT categories to accommodate dashboard plotting and alerts of abnormal activities for authorities, such as the GSP. The GSP dashboard provides a graphical view of the aggregate MVoT data, such as the trust score, distrust score, and message communication frequency. A separate analysis tool uses the MVoT data to provide a statistical analysis of threshold settings using hypothesis testing.

III. DTM Communications

A detailed representation of the DTM system and its communication pathways is shown in Figure 3. A Distributed Control Module (DCM) serves as a gateway between the DER and the GSP DER Management System (DERMS) server. This DCM provides encapsulated header information to the DTMC of all messages exchanged between itself, the DER and the DERMS. The DCM forwards these encapsulated messages to the DTMC. The DTMC message classifier then parses and classifies these messages. It then generates new MVoTs based

on the classified messages, which it then forwards to the CDTA.

When designing the DTM system, we ensure that the security applied to the network communication between DTM components over the network is secure. Hence, we implement the SEP security requirement to enable HTTPS. HTTPS network communication is enabled along three pathways: one between the DCM and the DTMC server, another between the DTMC client and the CDTA server, and the third between the CDTA and the GSP.

IV. DTM Dashboard and Messaging

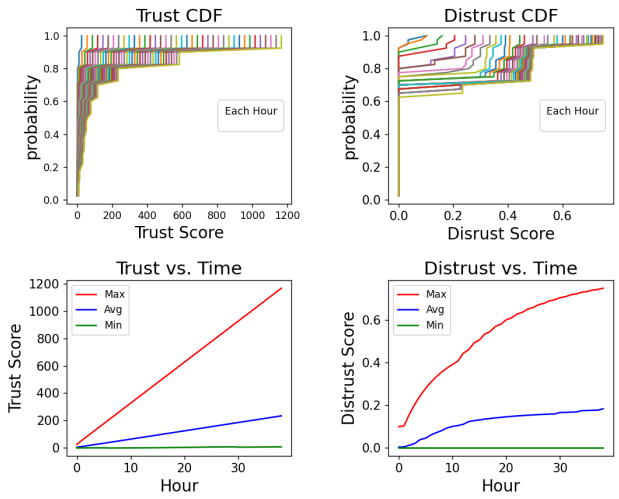


Fig. 2: The DTM dashboard showing the MVoT value trend over time.

The DTM dashboard provides the overall health of the EGoT network communication by displaying graphs of MVoT variable behaviors over time. Figure 2 shows a sample dashboard of the DTM system.

In our implementation of the dashboard, we provided flexibility to display a selective number of MVoT variable plots. Figure 2 shows the Cumulative Distribution Function (CDF) of trust and distrust, which are the overall trends in EGoT actors' trust values and distrust values over time. The dashboard can be expanded to include more MVoT variables. The CDF of MVoT graphs represents the probability of a specific MVoT value, such as trust score for a given time unit (e.g., hour). The MVoT plots, such as trust score over time, are critical plots for authorities who want to know the overall health of their EGoT system. The trust score versus time plot shows if there are increasing or decreasing trends in trust. Additionally, the graphical representation of distrust score versus time presents the trend in the mistrust of the system. This enables the observer to understand how many mistrustworthy incidents are happening within the EGoT network communication, independent of trustworthy incidents.

V. DTM Scaling Measurements

Testing for scalability is critical for the DTM system to ensure it can handle large amounts of data without impacting the storage capacity and the file processing time. The CDTA is susceptible to such issues. When measuring scalability, we looked at file process time and storage capacity in order to test the impact of scaling up. We used the Apache JMeter tool to mimic DTMCs from one unit up to 10,000 units, to send messages to the CDTA, and to observe the required process time and allocated memory space. Figure 4 represents the change in the processing time for the DTM Components Merger and Time Plot. We do not see a linear trend in the file process time, although we see an upward trend, as expected, when the number of DTMCs communicating with the CDTA increases. We observed that the cumulative processing time for the Merger script for 10,000 units was 43.2 seconds, and for the Time Plot, it was 552 seconds. In other words, the processing time of the scalability testing increased significantly as the number of clients increased to 10,000.

Figure 5 illustrates the second part of the scalability testing, the generated file size related to the increased scalability of DTMCs. For 10,000 DTMCs, we notice that the MVoT data files generated by the time plot script had a significantly larger file size than those generated by the merge script or the evaluated files containing trust scores reported by the CDTA. At the same time, both the Merge file script and the time plot required less than 25 MB of combined storage, which does not cause any storage issues due to file size.

VI. Hypothesis Testing for Setting Thresholds

Setting alert thresholds is critical to the DTM system. We developed the hypothesis test tool to analyze the MVoT calculations of the grid and help authorities, such as GSP, determine the tolerance level of abnormalities reported by the DTM system. This feature ensures authorities are not alerted for each incident of MVoT abnormality of just one or a few actors. Instead, the authority can set the tolerance level, and once the set threshold is passed, DTM system sends alerts reporting the specific abnormality trend. Figure 6 shows the output of our hypothesis test tool where Equal Error Rate (EER) and F-1 scores are shown with the variation in count threshold and value threshold. The count threshold is a predefined number that tells the tolerance for the count of actors with abnormal MVoT values threshold. The value threshold is a predefined number we used to determine if a MVoT variable value is abnormal when compared. The use of EER involves the observation of False Positive Rate (FPR) line and the False Negative Rate (FNR).

$$FPR = \frac{FP}{(FP + TN)} \tag{3}$$

$$FNR = \frac{FN}{(FN + TP)} \tag{4}$$

$$F1 = \frac{TP}{TP + 0.5(FP + FN)} \tag{5}$$

In these equations, False Positive (FP) is the count of false positive, True Positive (TP) is true positive, False Negative (FN) is false negative, and True Negative (TN) is true negative.

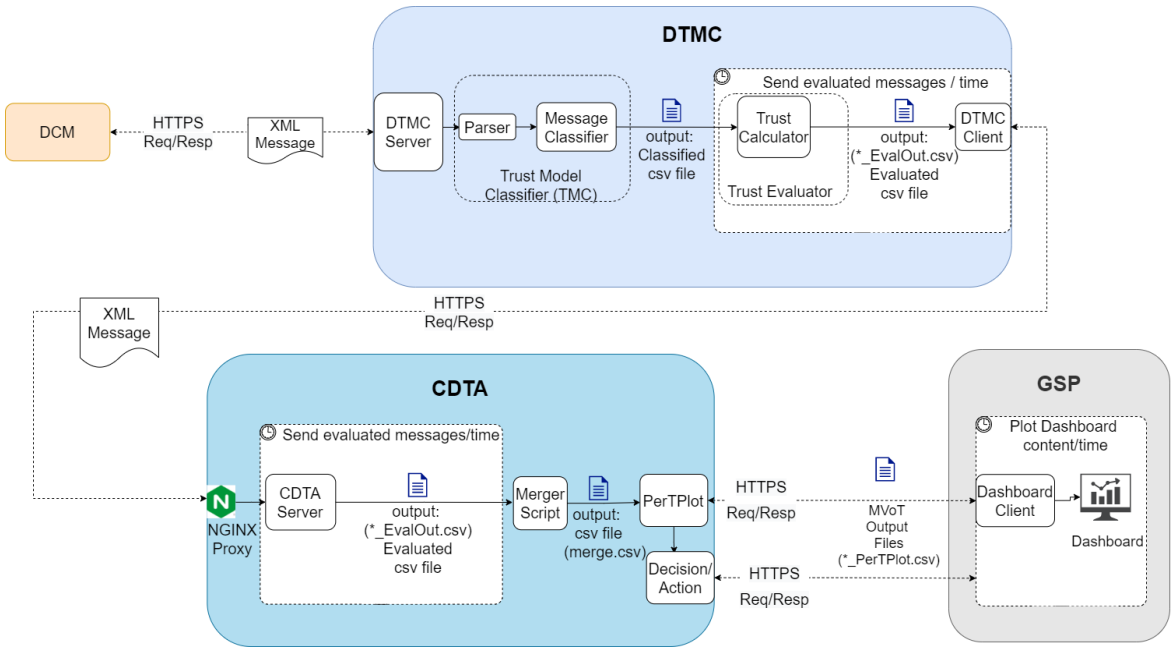


Fig. 3: Detailed representation of the DTM System described in this paper

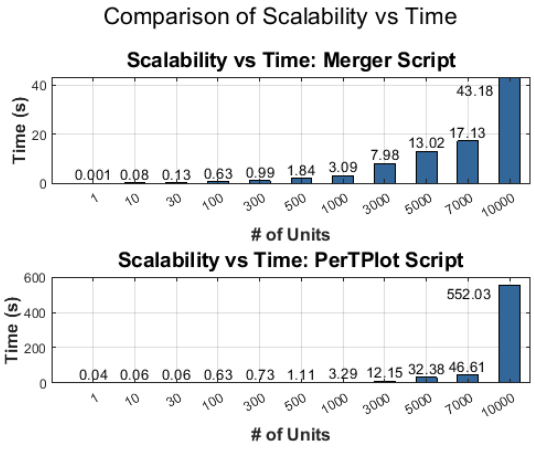


Fig. 4: The trend in file process time at the CDTA in reference to scalability.

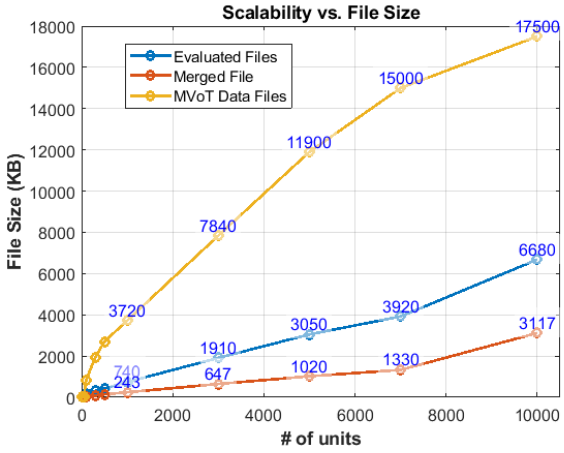


Fig. 5: The trend in file sizes at the CDTA in reference to scalability.

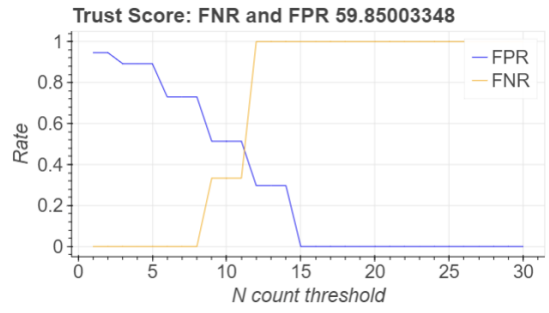
EER is the point where these two lines intercept. The significance of EER is the balancing point where the rate of sending false alerts and failing to send alerts are equal. The hypothesis test tool provides the GSP with a visual representation that helps decide to send too many alerts or hold off until a significantly large amount of abnormalities are present before alerting the GSP.

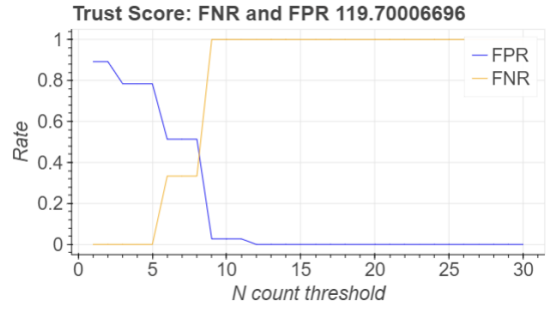
Once these thresholds are determined and provided, the DTM uses these values to determine when to send alerts. The hypothesis test tool is set to analyze all the MVoT values and help an authority decide on the threshold for each. The F-1 score is another statistical analysis we added to the hypothesis test tool. It is the harmonic mean of precision and sensitivity. The F-1 score, the FPR, and the FNR are used by the authority to adjust thresholds for the MVoT levels that trigger messages. Lower thresholds will mean more messages and increased false alarms; higher thresholds will mean fewer messages and increased missed alarms. Initially, the DTM will set the thresholds for an equal error rate to balance the FPR and the FNR. It is up to the authority to evaluate the most effective levels for their specific situation. Examples of alert messages sent from the DTM-System to the GSP:

- "Excessive time since last communication from GSP"
- "Excessive time since last communication from DER"
- "Trust is low for GSP"
- "Communication rate is low from GSP"

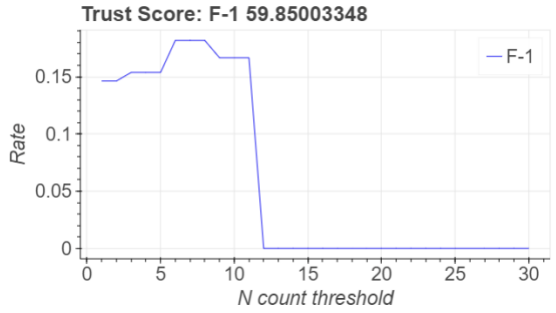
VII. Summary and Conclusions

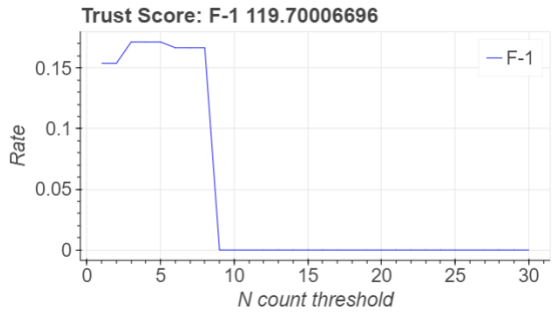
This paper presents implementing and evaluating a distributed trust model for the EGoT. The distributed trust model alerts EGoT participants that potential communication attacks may occur. The method to set and adjust thresholds for sending





(a)





(b)

Fig. 6: The hypothesis test tool shows the analysis of the Trust Score count threshold values of 59.85 and 119.7 for (a) FNR vs. FPR and (b) F-1 Score.

these messages is described. The idea is that trust monitoring can provide information protection against and early detection of unforeseen attacks.

VIII. Glossary

ACL Access Control List
AES-CCM Advanced Encryption Standard Cipher Block Chaining - Message Authentication Code
APT Advanced Persistent Threats
CDF Cumulative Distribution Function
CDTA Central Distributed Trust Aggregator
CSV comma-separated values
CTA Consumer Technology Association
DCM Distributed Control Module
DER Distributed Energy Resources
DERMS DER Management System
DS Distrust Score
DTM Distributed Trust Model
DTMC Distributed Trust Model Client
EER Equal Error Rate
EGoT Energy Grid of Things
FNR False Negative Rate
FPR False Positive Rate
GO Grid Operator
GSP Grid Service Provider
HTTPS Hypertext Transfer Protocol Secure
MVoT Metric Vector of Trust
SPC Service Provisioning Customer
TS Trust Score
TSLC Time Since Last Communication

References

[1] S. Widergren, R. Melton, A. Khandekar, B. Nordman, and M. Knight, "The Plug-and-Play Electricity Era: Interoperability to Integrate Anything, Anywhere, Anytime," *IEEE Power and Energy Magazine*, vol. 17, no. 5, pp. 47–58, 2019.

[2] T. Slay, J. M. Acken, and R. B. Bass, "Incentivizing distributed energy resource participation in grid services," in *2022 IEEE Conference on Technologies for Sustainability (SusTech)*, 2022, pp. 86–91.

[3] M. Obi, C. Metzger, E. Mayhorn, T. Ashley, and W. Hunt, "Nontargeted vs. Targeted vs. Smart Load Shifting Using Heat Pump Water Heaters," *Energies*, vol. 14, no. 22, p. 7574, 11 2021. [Online]. Available: http://dx.doi.org/10.3390/en14227574

[4] K. Marnell, C. Eustis, and R. B. Bass, "Resource Study of Large-Scale Electric Water Heater Aggregation," *IEEE Open Access Journal of Power and Energy*, vol. 7, pp. 82–90, 2020.

[5] IEEE Common Smart Inverter Profile Working Group, "Common Smart Inverter Profile: IEEE 2030.5 Implementation Guide for Smart Inverters," IEEE, Tech. Rep., 2018.

[6] "IEEE Standard for Smart Energy Profile Application Protocol," *IEEE Std 2030.5-2018*, pp. 1–361, 2018.

[7] A. Abdui-Rahman, S. Hailes, and S. Hailes, "A Distributed Trust Model," in *New security paradigms*, 1997, pp. 18–60. [Online]. Available: files/124/Abdui-Rahman et al. - A Distributed Trust Model.pdf

[8] Y. Kim, S. Hakak, and A. Ghorbani, "Smart grid security: Attacks and defence techniques," pp. 102–123, 2023.

[9] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet of Things*, vol. 14, p. 100111, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660519302148

[10] N. S. Fernando, J. M. Acken, and R. B. Bass, "Developing a Distributed Trust Model for Distributed Energy Resources," in *2021 IEEE Conference on Technologies for Sustainability (SusTech)*, 2021, pp. 1–6.

[11] M. Alsaid., N. Bulusu., A. Bargouti., N. S. Fernando., J. M. Acken., T. Slay., and R. B. Bass., "Privacy-preserving Information Security for the Energy Grid of Things," in *Proceedings of the 11th International Conference on Smart Cities and Green ICT Systems - SMARTGREENS*. SciTePress, 2022, pp. 110–116.

[12] M. Obi, T. Slay, and R. Bass, "Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards," *Energy Reports*, vol. 6, pp. 2358–2369, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484720312853

[13] N. S. Fernando, Z. Zeng, J. M. Acken, and R. B. Bass, "Trust Model System for the Energy Grid of Things Network Communications," in *2023 IEEE Conference on Technologies for Sustainability (SusTech)*. IEEE, 4 2023, pp. 280–287.