2023 IEEE PES Grid Edge Technologies Conference & Exposition (Grid Edge) | 978-1-6654-6012-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/GridEdge54130.2023.10102745

Security and Trust Metrics for Edge Computing

John M. Acken, PhD
ECE Department
Portland State University
Portland, OR, USA
acken@pdx.edu

Naresh K. Sehgal, PhD
NovaSignal Corp.
Cloud Engineering
Los Angeles, CA, USA
nareshksehgal@gmail.com

Divya Bansal, PhD
Cyber Security Research Centre
Punab Engineering College
Chandigarh, India
divya@pec.edu.in

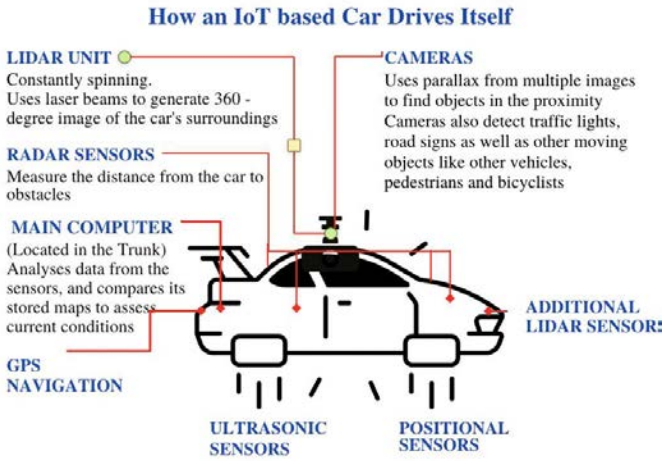
Robert B. Bass, PhD
ECE Department
Portland State University
Portland, OR, USA
robert.bass@pdx.edu

***Abstract*— The present state of edge computing is an environment of different computing capabilities connected via a wide variety of communication paths. The energy grid is relying upon distributed energy devices connected at the edge of the internet. Consider the scenario where each edge device is customer-owned distributed energy resource (DER) that is connected via a trustworthy link to a grid service provider. Each DER keeps a local simple trust record of interactions. Information protection is provided by internet https standards, however, trust must be evaluated throughout operation. This paper presents a model for representing and evaluating trust in general and applied to the energy grid as a key example. Actors on the edge may interact with each other as well as with a central datacenter.**

Keywords-Edge Computing, Security, Adaptive learning, Trust model, Threats, Cloud Computing, Information Security

I. Introduction

Edge computing represents a combination of distributed computing connected to centralized servers. Security considerations must include multiple subtopics, e.g., protecting information content from observation and alteration, protection of operational capability from unauthorized access, protection of normal operation in the presence of malicious overloaded requests, etc. Management of the data flow in general is described in a Common Information Model (CIM), which is an industry standard that defines device and application characteristics so system administrators and management programs can interface devices and applications from different manufacturers. A CIM provides for the protection of information flowing through the internet. However, this paper addresses the trustworthiness of that data flowing between actors. Actors on the Edge may interact with each other as well as with a central datacenter. Therefore, establishing trust in edge computing requires a distributed solution. Solution components need to consider prevention from and responses to any security threats [1]. Examples of prevention include encryption to protect content from observation and alteration, access checking protocols to prevent unauthorized accesses, tracking mechanisms to identify attempted attacks, and blocking messages except from trusted devices. Consider the power grid with many independent intelligent devices distributed among the customers. The basic concept is that customer-owned distributed energy resource (DER) are connected to through trustworthy links to a grid service provider (GSP). Each DER keeps a local simple trust record of interactions that allows the device to respond appropriately to requests. The request response is based upon the trust level between the requesting and the receiving device and can be one of: comply with request, ignore request, or send potential attack alert to appropriate monitor. Our proposal is that no single evaluation of trust is sufficient, but several evaluations of trust by each distributed actor are needed.



II. Emergence Of Edge Computing

Today's information technology environment contains a wide variety of computing resources and a multiplicity of communication channels. The high levels of security examples include hacking a hospital database, accessing banks, or operating factories.

With many IoT devices and use cases, it is imperative to have localized compute power and data storage. An example is a car [2], as shown in Fig 1, which can generate up to 5 TB of data/day. These data may come from onboard cameras, IR sensors, and measurements collected from the engine, brakes, etc. However, an autonomous car on the road cannot wait for a server in the cloud to make a decision to accelerate or brake. Hence, it needs sufficient compute power onboard to drive safely. This capability has been dubbed as a

978-1-6654-6012-5/23/$31.00 ©2023 IEEE

"data center on the wheels." The car can synch up with a remote data center in the cloud while parked. But on the road, the car must focus on safe driving with real-time decision-making. Hence, a part of the cloud is migrated from remote data center to the field, termed as edge computing.

However, some functions are still best guided from a central server, such as navigational decision for routing to a destination. The server can guide the car on which exit to take, but the onboard computer in a self-driven car must decide when to turn the wheels to take that exit.

Fig 1: A car's self-driving system with multiple sensors [2]

Similar examples can be found in other application domains [3] [4], such as smart homes with security cameras, which can distinguish an intruder from a family member or a stranger to sound an alarm [5].

III. Status of Edge Computing Security and Recent Breaches

Security concerns abound with the emergence of edge computing. In the car example, its computers are not behind a firewall but physically accessible to many people besides the owner. When a car is taken to a mechanic for an oil change or another repair, there is a risk of someone tampering with the hardware or software components setting up a future failure of the self-driven car. It is also possible for someone to access private data stored in the car, e.g., its travel points. Vulnerabilities in other unprotected devices such as home appliances (TV, fridge) on a network can be used to launch a cyberattack. A recent DDOS (distributed denial-of-service) attack was launched using hijacked home security cameras, while in another instance private video clips were stolen and posted on the Internet [5].

Even a simple home automation system, such as an intelligent door lock, needs the following security features for safety:

1. A firewall to dissuade remote hackers with login authentication.
2. Identification authentication of phone numbers, password, or biometrics, such as face recognition, thumbprint, retina scan, etc.

Note that any single biometric can be easily defeated, e.g., a pictured mask to fool a face recognition or copy of a thumbprint image, presented to the door camera. It is desirable to have a multifactor authentication system, but even this method has its shortcomins. Furthermore, a data-logging system is needed to record who opened or locked the door and when. These data are immediately backed up to a remote cloud server to avoid local tampering. Machine intelligence can be used to create a regular usage pattern and flag anomalies, e.g., when a door is opened at unexpected hours or with unusual frequency.

IoT devices periodically collect data about an environment or individuals, which can be potentially shared with third parties compromising privacy. It can range from personal preferences of Web browsing habits, TV channel selection, or images from home security cameras. Some devices can be programmed to selectively transmit data to a cloud service for processing, e.g., a security camera which has a buffer of 15 seconds but records and transmits a 30-second clip only if an event activity is detected, for 15 seconds before and 15 seconds after the occurrence of event. This reduces storage requirements but increases chances of a mistake, e.g., in motion detection. Such devices are designed to render service with minimal intervention, and yet they need to be directed using voice activation or image recognition for proper motion detection.

To ensure trust in edge computing a system designer starts with a trusted environment, trusted protocols, and tamper-proof components.

IV. Security Solutions using distributed actors

For information security purposes, an actor can be a person or an electronic digital device. Any given actor can have interactions with a variety of other actors for different purposes. Example types of interactions include financial, medical, machine control, etc. Each transaction for a type of interaction has different levels of security requirements and expectations, depending upon the relationship of the actors. Clearly, different types of interactions are appropriate for different types of actors. This environment of diverse and distinct interests in multiple systems precludes a system wide solution to security. Each system will have its own information security implementation. However, for an actor to function within the various systems, it must evaluate trust for the other actors in any specific transaction.

The evaluation needs a distributed trust model (DTM) that locally evaluates trust. Within a DTM, a message or transaction first enters a classifier block. From a trust perspective the message is evaluated as positive or negative based upon the relationship to the sender, the timing of the message, the margin of the values, and the specific request or response being made. Based upon the classification of the current transaction and the history of past evaluations, a trust score is then calculated and updated as both a trust level (TL) and a mistrust level (MtL). The history also includes past message data such as frequency of transactions, values of past transactions, and other metrics on timing of communication. Based upon the trust calculation and the level of security for the given relationship, the action decision block sends an appropriate response to the transaction. The responses could be to allow the transaction, to block the transaction, or to send

978-1-6654-6012-5/23/$31.00 ©2023 IEEE

an alert or to raise an alarm. These steps are shown in Figure 2. Calculation of TL and MtL are shown in Figure 3.

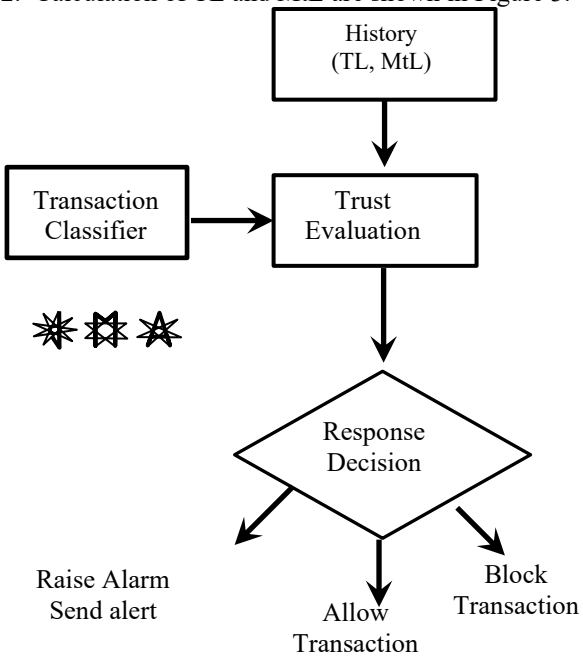


Figure 2. Generic steps for information-based trust evaluation for messages and transactions in a DTM system.

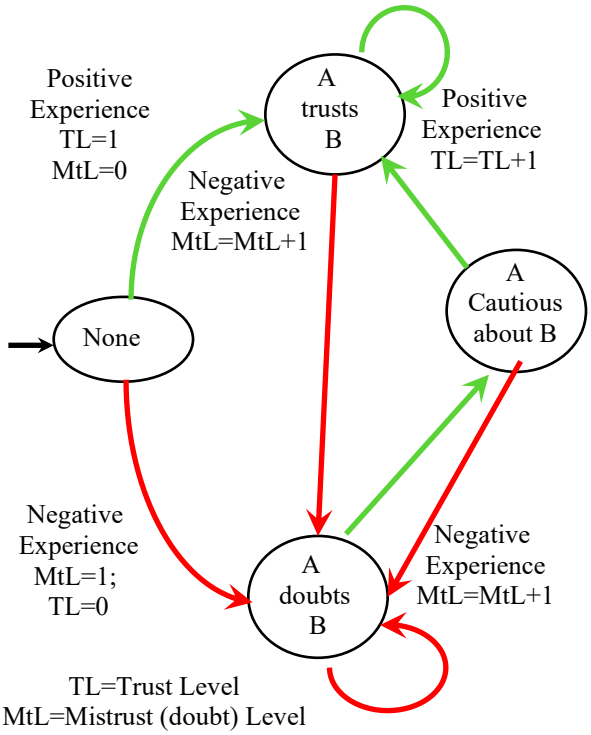


Figure 3. Generic calculation for information-based trust evaluation for messages and transactions.

A DTM creates separate trust values for each actor in relationship to each of the other actors. For example, a customer will have trust scores for their employer, the bank teller, the bank ATM, the bank server, and each vendor. Conversely, the bank teller will have a trust score for customer A, Customer B, the bank server, and the ATM. The trust scores are not equal in both directions. For example, customer A may have a high trust score for the vendor, but the vendor may have a lower trust score for customer A.

Let us apply the generic DTM to some specific examples. Consider a bank with actors that include a bank teller, the bank server computer, the bank ATM, multiple customers (C_A, C_B, C_C, …), multiple customer employers (E_A, E_B, E_C, ...), and multiple vendors (V_A, V_B, V_C, …). Consider that customer C_A initiates a purchase from vendor V_A. Vendor V_A initially classifies the request based upon verifying the bank card. Vendor V_A sends a funds request to the bank, the bank classifies the request based upon the customer's account, checks if the amount is within the withdrawal limit, classifies the transaction as positive, and finally, the evaluation of trust for vendor V_A and customer C_A is incremented by 1.

First, let us consider a bank and its relationships with customers. A customer will start by opening an account. The bank checks some credentials, and the customer gives the bank some money. This first transaction sets the Trust Level for the bank trusting the customer to 1. The customer doesn't really have a transaction to measure trust yet. The customer contacts the employer to create a direct deposit to the bank. After payday the customer sees the account balance has increased. This transaction increases the bank's trust of the customer by 1 and increases the customer's TL by 1. Next let us consider if the customer loses their bank card and someone else tries to use it. After the ATM marks the failed attempts, the card is blocked, and the bank increase the Mistrust level (MtL) by 1. The customer reports the card missing and the bank recognizes the report as a positive transaction and the TL increases by 1. But notice the MtL still has a negative mark. This is important in maintaining caution on the part of the bank. That is, a positive result does not automatically cancel a negative result. Trust is different for different purposes. Figure 4 shows the bank trust relationships. For the bank example, all the trust transactions are financial. However, note that with increasing number of players, the model states will grow exponentially if these players can also interact with each other. An example is if a bank allows one customer to have an authorization to operate another customer's account. Currently, this is limited by a bank, e.g., to minors in a family to keep its risks contained.

978-1-6654-6012-5/23/$31.00 ©2023 IEEE

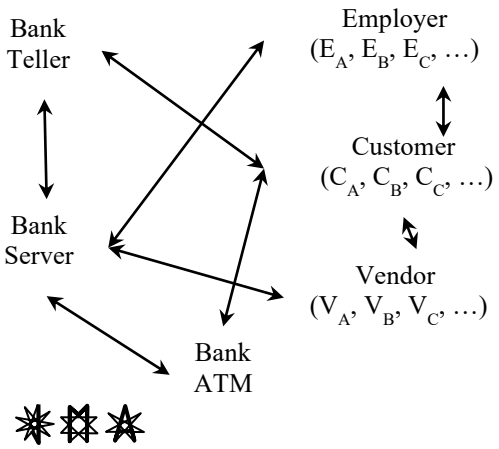


Figure 4. Bank relationships for trust evaluation.

Now consider the case of a hospital. Here there are two types of trust relationships. One is financial, so that billing and payments are the areas of concern. Another case is medical information and advice. So, while a patient will set a TL for the doctor based upon the care given, the patient will have two separate trust levels for the hospital. One trust level will be based upon the medical information, interaction with the equipment, and the care received. Another trust level will be based upon billing, dealing with insurance, and payment experiences. So, while the hospital will trust the bank and share relevant patient information needed to do financial transactions it is by law not allowed to trust the bank with any private health information. Figure 5 shows the hospital trust relationships.

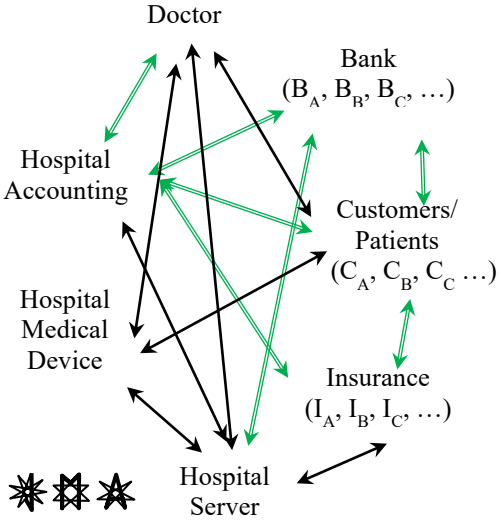


Figure 5 Hospital relationships for trust evaluation.

Now consider the case of an individual house participating in a smart energy grid. This is where a customer's energy device (such as an electric car or an electric hot water heater) can be utilized by the grid as a DER. The customer contracts with a GSP to allow the GSP to coordinate the operation of DERs with the Grid Operator. This provides efficient and reliable energy on the grid while providing financial incentives to the participants. Figure 6 shows the trust relationships for a smart energy grid.

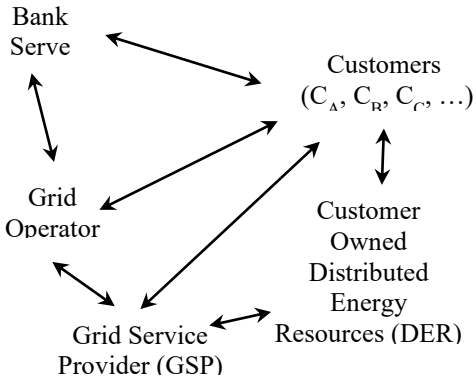


Figure 6. Smart Energy Grid relationships for trust evaluations.

V. Security Modelling Specifically Evaluating Distributed Trust

Perimeter defense has long been insufficient for IoT security. Fixed protocols for boundaries of security with individual devices' security implementations will fail.

Let us consider an example of applying the previous trust model calculations from the perspective of the customer/patient. The medical world is working to include health monitoring with edge computing [6]. First, consider the case of a patient and physician. Table I shows the current trust evaluations between a patient/customer and several entities. The trust scores are updated based upon the diagrams described in the previous section. The table shows the trust score for the trust by the customer of the entity and the trust scores for the entity trusting the customer/patient. Each score is an ordered pair of Trust level and Mistrust Level (TL, MtL). Now consider that a patient wishes to get a prescription. A message is sent to the Doctor. Because the patient has an established level of trust for this patient, in this case (20,0), the doctor forwards a message to Insurance. Notice that the trust level between the doctor and the patient is asymmetric. That is the patient has a higher trust of the doctor than the doctor has of the patient. This can come about because there are fewer messages from the patient to the doctor than from the doctor to the patient. However, Hospital insurance has had no past problems with this customer and in this case the trust scores are (5,0). This transaction fails requiring further action.

The previous discussions concentrate on the pair wise trust level between two entities. However, in reality there are multiple entities involved in some trust relationships. As an example, some security protocols include a third-party security certification. In addition, there are some security situations where a third-party monitors or records

978-1-6654-6012-5/23/$31.00 ©2023 IEEE

transactions. These considerations will be explored in future work. The application of Deep Learning for speech recognition is advancing [7], and it could be applied for speaker recognition for authentication and other security evaluations. The concept is to push some of the security decisions to the edge computing devices. The additional compute power at the edge is already being applied for decision making using machine learning [8][9].

Table 1. Example trust calculation score between a customer and bank's entities. Scores are ordered pairs of Trust level and Mistrust Level (TL, MtL). Each entry has two sets of trust scores, the customer's trust of the entity and the entity's trust of the customer. The pair of (0,0) means no trust has been established.

	Financial	Medical	Energy	Casual
Doctor	{(5,0), (5 ,0)}	{(20,0), (40,0)}	{(0,0), (0,0)}	{(5, 0), (0 ,0)}
Hospital server	{(10, 0), (10,0)}	{(5, 0), (5,0)}	{(0,0), (0,0)}	{(0,0), (0,0)}
Insurance	{(5,0), (5 ,0)}	{(10, 0), (10, 0)}	{(0,0), (0,0)}	{(0,0), (0,0)}
Hospital Accounting	{(10,0), (15 ,0)}	{(0,0), (0,0)}	{(0,0), (0,0)}	{(0,0), (0,0)}

The future of security with edge computing and the cloud is a mix of central protocols in the cloud, decision making at the edge based upon machine learning, monitoring and analyzing communication activities [1]. A machine learning environment may allow the identification and defense against unexpected and unpredictable security challenges [10].

VI. Future Work

It is worth recapping that there are still many unsolved open challenges in realizing a robust trust scoring algorithm for edge computing. It is crucial to identify and analyse these challenges and seek novel theoretical and technical solutions. With this view, we discussed some prominent challenges in attaining secure and a trustworthy scoring system.

In an ecosystem where an entity has existed for some time, a new interaction with a new entity can reuse previous learnings from other systems to start with a non-zero trust state. For example, a lender often checks credit history of an applicant and based on their past transactions with other entities and systems to determine the loan worthiness of the new applicant. This can be leveraged in case of distributed devices too, if one device is allowed to access the trust history of other participants. In the specific instance of health care, patient health information is protected by HIPPA with stiff penalties [11], but a care giver's history is available to the patients to make their informed decisions.

In our present model, we have considered that the level of Trust in the state diagram changes to positive experience and increments the Trust Level (TL) by 1. Another idea is to not increment Trust or Mistrust levels by 1 every time, this can be a fractional value between 0 to 1. This can be determined by dynamic weights, which are learnt behaviors and change over time. Because, in real life, metric termed Trust Score metric should measure for the trustworthiness which should vary dynamically with respect to time and be based on several functions comprising of parameters namely persistence, competence, reputation, credibility and integrity [12]. The value of trust scores lie between 0 and 1 with each parameter to measure trust is normalised to the unit value.

At present, the proposed trust model is assumed to work in a single ecosystem with no trusted third party available. To realize a more practical model, it should be adaptable to multiple entity environments, where the same experience can be interpreted by different entities in different ways. This is especially true if these entities are not purely logical and objective, e.g., cognitive biases that build upon time and are subjective in nature. The dataset presented to train ML based models can make a huge impact on the trust scoring system. A recent study done at MIT showed how AI systems can reinforce existing biases and exclusions [13].

As a part of the study, three different face-recognition systems were tested, and it was found that the accuracy is best when the subject is a lighter skinned man. Since the facial recognition software is being used by Law Enforcement Agencies to identify suspects, inaccuracies could lead to systematically ingraining biases in police stop and searches. Studies have thus shown that we need to take into account data diversity [14].

A future evolution of our model will look into when it is permissible to bring in past transactions of an entity to its new pair of relationships and when it is not. An example of a more complex trust calculation that is applied to the smart energy grid is a metric vector of trust [15].

VII. Summary

The present state of edge computing is an environment of vastly different computing capabilities connecting via a wide variety of communication paths. This situation creates both great operational capability opportunities and unimaginable security problems. This paper emphasizes that the traditional approaches to security of identifying a security threat and developing the technology and policies to defend against that threat are no longer adequate. We proposed a distributed trust model comprising of trust and mistrust scores. The wide variety of security levels, computational capabilities, and communication channels require a learning, responsive, varied, and individualized approach to information security. We propose that each element in the edge computing world use a localized ability to establish an adaptive learning trust model with each entity that communicates with that element.

References

[1] N. K.Sehgal, S. Sohoni, Y. Xiong, D. Fritz, W. Mulia, and J. M. Acken, *"A cross section of the issues and research activities related to both*

978-1-6654-6012-5/23/$31.00 ©2023 IEEE

information security and cloud computing," IETE Technical Review, Volume 28, Issue 4 [p. 279-291], 2011.

[2] Awais, Muhamad, and Asif Mehmood. "*Artificially Intelligent Self-Driven Car with Obstacle Avoidance*." LC International Journal of STEM (ISSN: 2708-7123) 1.1 (2020): 7-9.

[3] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). *Internet of Things (IoT): A literature review. Journal of Computer and Communications*, 3(05), 164.

[4] Gokhale, Pradyumna, Omkar Bhat, and Sagar Bhat. *"Introduction to IOT*." International Advanced Research Journal in Science, Engineering and Technology 5.1 (2018): 41-44.

[5] Dange, S., Chatterjee, M. (2020). *IoT Botnet: The Largest Threat to the IoT Network*. 10.1007/978-981-15-0132-6.

[6] Hamilton, W. L., et al. *Loyalty in online communities*. Proceedings of the eleventh international AAAI conference on Web and Social Media (ICWSM 2017), pp. 540–543.

[7] Deng, L. et al. (2013). *Recent advances in deep learning for speech research* at Microsoft. 2013 IEEE int. conf. on Acoustics, Speech and Signal Processing, Vancouver, BC, pp. 8604–8608. https://doi.org/10.1109/ICASSP.2013.6639345.

[8] Nelson, R. (2017, June). *Smart factories leverage cloud,* edge computing. Evaluation Engineering, 56(6).

[9] Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020, *April*). *Machine learning and deep learning techniques for cybersecurity: a review*. In The International Conference on Artificial Intelligence and Computer Vision (pp. 50-57). Springer, Cham.

[10] Sfar, Arbia Riahi, et al. *"A roadmap for security challenges in the Internet of Things.*" Digital Communications and Networks 4.2 (2018): 118-137.

[11] Nahra, K. J. (2008). *HIPAA security enforcement is here*. IEEE Security & Privacy, 6(6), 70-72.

[12] John Joseph, Adri Jovin and Marikkannan Mariappan. "*A novel trust-scoring system using trustability co-efficient of variation for identification of secure agent platforms.*" PLoS ONE 13 (2018)

[13] B van Giffen, Dennis Herhausen, *Overcoming the pitfalls and perils of algorithms: A classification of machine learning biases and mitigation methods*, Journal of Business Research 144(6):93-106, May 2022

[14] Gong, Zhiqiang, Ping Zhong, and Weidong Hu. "*Diversity in machine learning.*" IEEE Access 7 (2019): 64323-64350.

[15] N. S. Fernando, J. M. Acken and R. B. Bass, *"Developing a Distributed Trust Model for Distributed Energy Resources,"* 2021 IEEE Conference on Technologies for Sustainability (SusTech), 2021, pp. 1-6, doi: 10.1109/SusTech51236.2021.946

978-1-6654-6012-5/23/$31.00 ©2023 IEEE