Al-Nahrain Journal for Engineering Sciences

Al-Nahrain J. Eng. Sci. 29(1) 174-180, 2026
Original Article

Cyber security for smart inverters and distributed energy resources (DER)

Qaeser Mohsen Khayoon [1]●, Hassan Hadi M.A Al-Fatlawi [2]● and Ali Jasim Albhadly [3]●

1,2,3Ministry of Oil, Petroleum Research and Development Center (PRDC). Baghdad, Iraq

●*These authors contributed equally to this work*

DOI: http://doi.org/10.29194/NJES.29010174

Received: March 20, 2025 **Revised:** May 16, 2025 **Accepted:** July 20, 2025 **Published:** March 20, 2026

Abstract

The growing use of "distributed energy resources (DER)" will result in a significant increase in the total number of gadgets or devices that users and third parties own and control. These gadgets rely largely on digital communication and control, placing them in danger due to cyber threats. This study presents a comprehensive framework that is resistant to attacks for defending integrated DER and major power grid infrastructure from hostile cyber-attacks, ensuring the safe integration of DER without jeopardizing system dependability and stability. This research focuses on the development of a cyber-physical power system that incorporates a significant integration of DER and analyses the particular cyber security problems brought about by DER integration. Following that, we provide a systematic DER resilience analysis approach, in addition to effective and measurable resilience measurements and concepts concerning design, and we summarize important DER assault scenarios. In conclusion, we suggest preventive, detective, and responsive measures against cyber-attacks, specifically tailored for integrating Distributed Energy Resources (DER) throughout the physical, cyber device, and regulatory levels of an eventual smart grid.

Keywords: *Distributed Energy Resources (DER), Cybersecurity, Resilience Analysis, Cyber-Physical Power System, Smart Grid Integration.*

Corresponding author: Provide the corresponding author information and publisher here. E-mail address: mohsencaeser@gmail.com

1. Introduction

Solar energy is one among various power generation technologies employed in the grid. It plays a role in extensive power generation through solar farms and large-scale installations and in smaller-scale distributed energy resource (DER) generation through grids, storage systems, and, rooftop installations. Solar energy is a type of DER technology that generates and distributes electricity on a local and large scale. Solar energy systems link to the electrical grid through power electronic devices like inverters, and they might establish duplicate communication channels with utility control and automation systems [1,2].

Before large-scale solar energy systems can be put into operation, they must meet critical infrastructure protection standards. Smaller PV systems and other DERs, on the other hand, currently lack cyber security requirements and are typically connected to the Internet by their owners for monitoring and control. As renewable energy infrastructure becomes a more popular target for cyber – attacks, cyber security becomes a critical concern for grid operators and solar system owners in protecting linked electric power networks from digital attacks.

The importance of cybersecurity extends beyond its apparent role in web usage, safeguarding data, and technological progress. Its significance also lies in areas such as policy formulation, legal safeguards, healthcare, and education [3,4] The inherently interdisciplinary nature of cyber security makes it difficult to define precisely. (Cyber security is the organization and gathering of resources, procedures, and structures to secure cyberspace and cyberspace-enabled systems against events that misalign de jure from de facto property rights. This definition was reached by [5] Given the widespread nature of online interactions in contemporary society, experts recommend the adoption of a unified public security philosophy. This philosophy should articulate both the objectives, such as policy development, and the methods, including regulatory measures, to ensure and protect cybersecurity.

Attacks on IT and "the operational technology (OT)" networks can take numerous forms, but among the most common are spear phishing attempts, malware distribution with the goal of data encryption for ransom or disruption of operations, and manipulation of controllers' control logic through the use of commonly used ports and application layer protocols (6).

The consequences of such disasters involve a diminished ability for human operators to perceive, leading to operational disruptions

(unavailability), decreased productivity, and financial losses [7]. Decentralization is one of the three most prominent developments in energy operations, DE carbonization, and digitization.

Examples of energy-generating technologies that have gained widespread recognition in the last twenty years are wind and solar power producers. It is possible to include RES in the various power grids, including distribution, transmission, and consumer power. Distributed and customer-level connections are more common for small-scale and 'behind-the-meter (BTM)' RES, while transmission-level connections are more common for large-scale RES. While the primary revenue stream for Renewable Energy Sources (RES) comes from selling clean electricity, project owners can also derive additional benefits from related products like Tax credits for renewable energy and the trading of renewable energy certificates (RECs). Currently, involvement in renewable energy markets may require acquiring certificates of origin, like GOs in the EU, RECs in the US, and I-RECs globally. The NIST Smart Grid Cyber Security Controls were used to map the cyber security requirements for securing Renewable Energy Certificates (REC) applications and data. The "Cyber Security Frameworks" of the "National Institute of Standards and Technology (NIST)" are also used to suggest a cyber-security maturity model for securing REC data and applications. DLT is a perfect platform for such REC operations. Although Distributed Ledger Technology (DLT) aligns with current cybersecurity measures, implementing a Renewable Energy Certificate (REC) based on DLT which is a completely functional trading platform on the present power system and market necessitates thorough system changes [7].

It is advised that the intended use case be mapped at a more comprehensive resolution, taking into account the relevant power system, and frameworks for cyber security standardization and communication, before conducting actual experiments. Energy companies, and the electric power grid in particular, are becoming targets of more frequent and sophisticated cyberattacks [8].

A major cyber assault on the electricity system could lead to severe repercussions for grid operations, encompassing socioeconomic consequences, market effects, damage to equipment, and extensive blackouts. Several efforts, including the "Cyber Security Roadmap" and "Critical Infrastructure Protection (CIP) Standards", have investigated the security and resilience of the electrical system against cyber threats.

Five-level distributed energy resources (DER) system architecture was proposed [9,10]:

(1) DER production and storage on one's own

(2) Management of DER energy in a facility

(3) Operational communications between utilities and retail energy providers (REPs)

(4) Analysis of distribution utility operations

(5) Market and transmission activities.

Connecting a similar DER system design to the "European M/490 Smart Grid design Model (SGAM)" in "IEC 62351-12" facilitated extensive data interchange across various system levels.

Many different types of cyber-attacks might exploit the many holes in the ever-changing DER architecture [10,11]:

(1) First, many different types of energy equipment, such as "e.g., battery controllers and smart inverters," are owned and operated at different customer and utility locations due to the widespread use of DER. There may be many more distributed energy resource (DER) devices owned by consumers and linked to the grid than utilities.

(2) Due to the diverse security administrative domains covered by Distributed Energy Resources (DER), the utility's ability to oversee security extends only to monitoring devices up to the smart meter. DER owners are expected to manage their equipment independently.

(3) The many networks that regulate "Distributed Energy Resources (DER)" may be interconnected with other "Information Technology (IT)" networks and building automation networks, increasing the number of possible entry points. These three essential features bring a plethora of new dangers to DER and the grid as a whole—emerging Critical DER Security Challenges, as shown in Table 1.

Table 1. Critical Emerging DER Security Challenges [12].

Challenges of Security	Smart Meter/AMI	DER
Administration divided	The utility either possesses the complete "Advanced Metering Infrastructure (AMI)" system or engages a managed service provider. This guarantees the proper installation and configuration of relevant security procedures and updates. When purchasing systems, utilities also prioritize cyber security.	The owner of smart inverters will likely be the "Distributed Energy Resource (DER)" operator rather than the utility. The utility may lack the technical expertise or willingness to prioritize and uphold system security.
Increased Cyber-physical Interdependence	The cyber-physical interdependencies of smart meter attacks are restricted. In general, monitoring the grid's physics can identify only attacks that disconnect a meter.	Preventing, identifying, and mitigating hazardous DER operations will rely heavily on an analysis of both the grid's cyber and physical properties.
Increased Grid Impact	While the removal of meters will leave customers without power, it is unlikely to have a substantial influence on the distribution grid's dependability and stability.	If DER penetration is strong harmful action of smart inverters in the grid may have a substantial influence on the distribution grid by injecting excessive power or purposely changing voltage, jeopardising the bulk power system's stability.
Key Exchange & Cryptography	To simplify cryptographic methods and key exchanges must be implemented for securing connections, the utility either possesses the complete "Advanced Metering Infrastructure (AMI)" network or employs a managed service.	The networks must traverse several administrative boundaries for utility commands to manage the consumer-owned DER. As a result, many parties must exchange keys and revoke them.
Privacy	Utilities often receive meter readings at intervals of 15	Utilities can ascertain the condition of

	or 60 minutes, capturing data only on substantial load fluctuations.	"Distributed Energy Resources (DER)" within minutes or seconds. This information could be employed to develop more precise consumer profiles.
Additional Control Functions	Demand response and load disconnects are common features of smart meters.	Smart inverters offer complex control functions that can have a substantial impact on utilities and consumers' capacity to manage smart inverters.

To support DER, A varied combination of devices and networks is essential; however, prior research has only investigated a portion of this foundational interaction and its infrastructure. Numerous notable scientific projects, including [13,14,15]

(1) Smart meter security analysis.

(2) Smart meter intrusion detection methods.

(3) New security procedures for smart meters are being designed.

Even though secure smart meters are crucial for integrating "Distributed Energy Resources (DER)", the bulk of DER advancements take place "behind the meter". This involves incorporating new sources of energy and cyber-control systems. Furthermore, the control mechanisms required have to be adaptive between administrative domains "for example, between utilities and customers". This raises a slew of new cyber security issues in addition to those raised by smart meter deployments as shown in Figure 1.

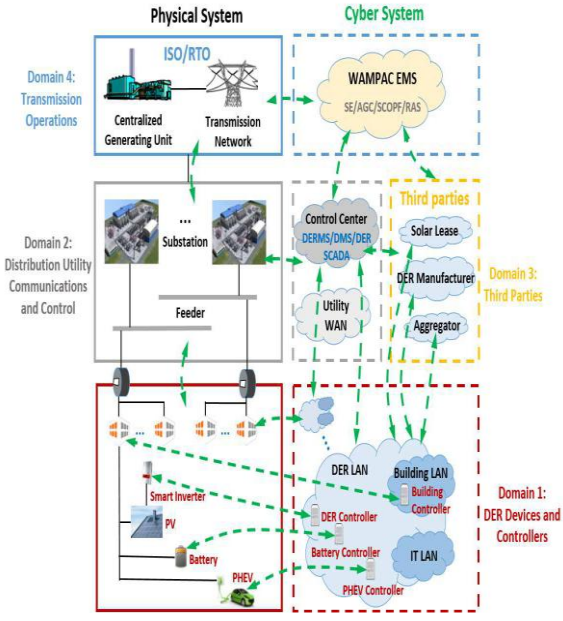

Figure 1. Architecture for DER Proposal [16].

2.Comparisons between recent studies and recent studies in cyber security for smart inverters and distributed energy resources

DER is growing in importance in the Smart Grid paradigm for power systems. DER security is becoming crucial since these systems increasingly rely on information and communication technologies. Many technologies have been proposed in the last few years for the protection of industrial control systems, ranging from cryptography, network security, security monitoring systems, and innovative control strategies resilient to cyber-attacks. Still, electrical systems and microgrids present their own peculiarities, and some effort has to be put forth to apply cyber-protection technologies in the electrical sector. In the present work, we discuss the latest advancements and research trends in the field of DER cyber security in a tutorial form

Many studies have examined the vulnerabilities of smart grids, specifically microgrids. This paper will discuss the most recent advances and new research trends in smart DER cyber security, as well as the applications of innovative technologies such as Software Defined Networking, new approaches for intrusion and anomaly detection, and resilient control strategies.

In the sphere of industrial processes, particularly in power systems, common anomaly detection algorithms rely on dynamic state estimates. Even if efficient, this method requires knowledge of the system's actual behavior. Machine Learning (ML) techniques could be beneficial in addressing this issue. In the realm of cyber-physical system anomaly detection, it is extremely usual not to have a dataset containing examples of poor physical behavior during a cyber-attack. As a result, it is necessary to use algorithms that can "learn" normal behavior and classify fresh samples.

The study concludes with a discussion of robust control techniques as an interesting research area. The control of electrical grids is critical for service continuity. Taking control of the electrical grid in both islanded and grid-connected modes can inflict significant damage and have an impact on the overall grid's stability. Resilience is required in this field. More research is needed to develop commercial items for usage in the field, although results from models and prototypes are quite promising.

3.Cyber security Framework for DER

As the developing snare of interconnected Appropriated Energy Assets (DERs) and savvy inverters raises worries about lattice steadiness, powerful digital actual security and flexibility measurements are pivotal. These measurements, safe to weaknesses and assaults, won't just form trust in DER use but additionally outfit utilities with information to pursue informed choices in regards to DER coordination and its possible effect on the network, at last making ready for more extensive reception by the two utilities and purchasers. [14,17]

1. Effect of DER capabilities on matrix dependability: This point digs into the center issue of what DERs mean for the lattice, establishing the groundwork for understanding potential security concerns.

2. Perceivability of malignant DER activities: Expanding on the laid-out influence, this point centers around distinguishing explicit weaknesses inside DER structures that could be taken advantage of for vindictive purposes.

3. Passable DER infiltration for lattice trustworthiness: At long last, with an unmistakable comprehension of both effect and weaknesses,

this point resolves the basic inquiry of how much DER mix can be permitted while keeping up with framework dependability.

The aforementioned concepts of design for security will outline fundamental security attributes for various messages and services related to "Distributed Energy Resources (DER)", encompassing aspects such as confidentiality, integrity, and availability. Subsequently, it will employ cyber-attack threat models and "Distributed Energy Resource (DER)" system architectures to assess the significance of threats and uncover tradeoffs among the level of integrated DER, control granularity, and infrastructure cybersecurity [18,19].

3.1 DER attack prevention:

Protecting the power lattice with a developing number of Conveyed Energy Assets (DERs) requires tending to their special network safety needs. This requires the plan and execution of hearty digital protection designs and cycles.

The center areas of center ought to be:

•DER access control models: Laying out secure doors and conventions for approved admittance and correspondence.

•Cryptographic exercises: areas of strength for executing, including key trade and the board, to safeguard delicate DER information and tasks.

•Confided in processing tasks: Using equipment and programming advancements that guarantee the uprightness and legitimacy of DER frameworks.

Moreover, identification systems should be utilized to distinguish both digital and actual assaults against DERs [14]. By proactively tending to these weaknesses, we can guarantee the protected and dependable reconciliation of DERs into the power network.

3.2 Detection of DER attacks:

Identifying and responding to malicious activity within Distributed Energy Resources (DER) is crucial for maintaining grid security. To achieve this, effective techniques must incorporate both cyber and physical components to detect irregularities and unusual usage patterns. By enhancing monitoring techniques and employing algorithms that reliably associate physical and cyber events, we can generate accurate indicators of potential attacks and provide actionable data for immediate utility response.

These algorithms will be fed with data collected from various utility infrastructures and DER domains within the control center. To enable effective response, attack detection methods must provide sufficient information about the threat, including:

•The list of affected DER resources

•The suspected malicious intent (e.g., voltage/frequency violations)

•An assessment of the severity

This revised structure prioritizes the importance of identifying and responding to malicious activity and then explains the steps involved in achieving this objective. Additionally, bullet points are used to highlight the specific information required for an effective utility response. [20,21]

3.3 DER Attack Response:

After identifying a digital assault on a Dispersed Energy Asset (DER), a quick and proper reaction is critical to limit lattice disturbance and guarantee framework security. The particular reaction will rely upon a few variables, including the DER's vindictive way of behaving, assault seriousness, and trust in the recognition.

•High-certainty assaults: For affirmed high-influence assaults, quick disengagement of the impacted DER from the network is the suggested game plan. This segregates the danger and forestalls further damage.

•Low-certainty occasions: Elective estimates like controlling contiguous DERs can be investigated for less certain circumstances. This approach expects to offset the adverse consequence of the possibly compromised DER without cutting off its association altogether.

•Persistent enhancement: Exploration is progressing to distinguish the ideal reaction methodologies for different assault situations, planning to give utilities an exhaustive tool compartment for addressing digital dangers to DERs [14, 22].

4. Modeling of Cyber-Physical Threats

To research the security weaknesses presented by DERs and brilliant inverters to power lattices, we distinguished two vital regions for reproduction and displaying:

1. Digital Danger Scene: Existing examinations [12,23] feature various digital dangers focusing on DER regulators, shrewd inverters, and their connection points with the lattice's Wide Region Checking Insurance and Control (WAMPAC) frameworks.

2. DER Control and Correspondence: The network safety stance of DER frameworks is vigorously affected by their control frameworks and correspondence conventions. These incorporate DER regulators, shrewd inverters, and battery regulators. To show these viewpoints really, we utilize digital engineering dialects like "information stream charts (DFDs)" and the "Building Examination and Plan Language (AADL)". Explicit subtleties to be displayed include:

•Correspondence conventions: Particular conventions used for DER control, for example, IEEE 1815 (DNP3), IEC 61850-7-420, SEP 2.0, and Modbus.

•Message geographies: Different correspondence structures utilized by DER frameworks, including unicast, multicast, and broadcast.

•Control capacities: Key highlights of brilliant inverter control, for example, volt-var the board, status detailing, recurrence watt the executives, and time synchronization.

3 – Grid and DER:

The distribution grid's physical properties, feeders, and integrated DER all have a significant impact on how attackers damage the grid's stability and reliability.

The modeling will encompass various components including energy storage for smart inverters, photovoltaic (PV) systems, capacitor banks, voltage regulators, and transformers, as well as protective elements like relays, re-closers, and fuses [24].

A key evaluation criterion involves determining the proportion of Distributed Energy Resources (DER) that can be incorporated into the grid while ensuring reliability in the face of cyber-attacks. Additionally, it is essential to take into account local aggregated controllers, such as microgrid controllers.

4 – Distribution and Transmission mixed with DER:

The integration of Distributed Energy Resources (DER) at a higher level will impact both the distribution and transmission grids. Furthermore, transmission grid disturbances can have an impact on a huge number of DERs in the distribution grid. Consequently, there is a need for integrated modeling and analysis of coupled transmission and distribution systems, along with improved power flow analysis that considers both transmission and distribution, incorporating Distributed Energy Resources (DER) [14,25, 26].
Figure 2. Illustrated threat scenarios against DER.

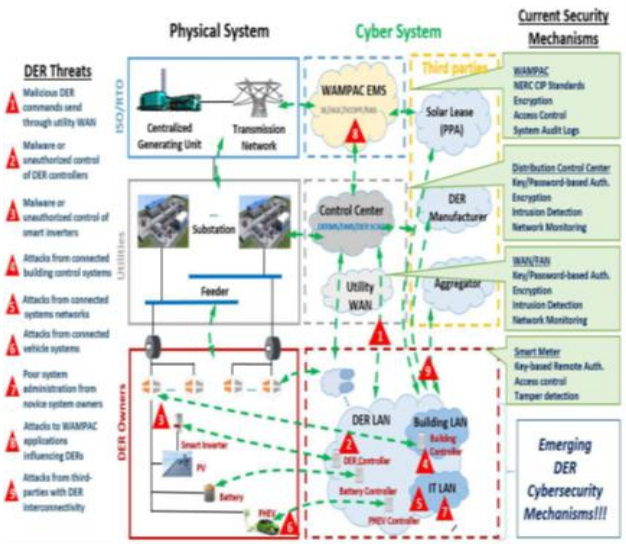

Figure 2. Threat scenarios against DER [16].

5. Framework for Renewables, DER, and Smart Inverters Cyber security

The proposed framework offers adaptability by offering tactics to identify, prevent, and react to an attack spanning the cyber, utility layers, and physical, ensuring the continuous operation of the network during a cyber assault [27, 28, 29]

1 – Cyber Layer Security.

The critical requirement for trustworthy DER gadgets: With utilities progressively depending on Disseminated Energy Assets (DER) for network control, getting these gadgets against digital dangers becomes central. Notwithstanding, the absence of direct regulatory command over various DER units presents a test in laying out trust for basic tasks.

Confided-in processing base for basic capabilities: Addressing this challenge requires DER gadgets to use a confided-in registering base (TCB) for safeguarding key control capabilities and delicate cryptographic tasks. Research endeavors in carrying out "Confided in Stage Modules (TPMs)" and "Confided in Execution Conditions (TEEs)" inside DER gadgets are significant in accomplishing this objective. These advances offer improved confirmation against programming weaknesses and aggressor admittance to basic framework information.

Moving past restricted adaptability arrangements: Customary methodologies depending on equipment security modules and secure co-processors with restricted adaptability probably won't be adequate. All things being equal, focusing on program detachment in light of criticality and utilizing Confided in Execution Conditions (TEEs) gives more noteworthy security while permitting future usefulness development. Instances of capabilities requiring seclusion include:

1. Key capacity and cryptographic tasks
2. Event inspecting and revealing
3. Setpoint administration

The subsequent enumeration explores possible entities and roles that could be utilized in constructing such a model.

2 –Manufacturer:

The manufacturer may ask for read-only access to operational data obtained from smart inverter performance to identify inefficiencies or flaws in the devices. Furthermore, to address some of these difficulties, the vendor may need to upgrade the devices' firmware.

3 – Consumer:

System settings, status information, and load data will require read-only access from the consumer. Because they are in charge of the first setup of the DER, they may choose to specify the smart inverter's operational settings. In addition, the consumer can restrict other owners' access to consumption data.

4 – Utility

To respond to various grid events, the utility may have to dynamically modify the parameters and set points of smart inverters to accommodate their reactions. Additionally, utilities require gaining access to the characteristics of the device to ensure the proper functioning of various Distributed Energy Resources (DERs) and to support other grid analytics purposes.

5 – Power Purchase Agreement (PPA)

As the outsider provider might claim and keep up with the PV exhibit, they will expect admittance to the framework and, subsequently, its creation information. This information will be used for a few essential purposes:

•Observing PV exhibit effectiveness: They'll follow execution and recognize possible issues to enhance energy creation.

•Assessing cost/energy investment funds and techniques: Information investigation assists gauge with costing reserve funds and illuminates effective framework activity procedures.

•Evaluating existing settings and boundaries: Tweaking framework settings for ideal execution requires bits of knowledge of the current arrangement.

•Client charging: Assuming the provider charges in light of energy creation, exact information is fundamental for fair charging.

5.1. Detection of Cyber Layer Attacks

DER digital assault discovery methods should adjust existing savvy lattice techniques to the remarkable correspondence and control conventions of these circulated assets. While checking utility-controlled network associations and gadgets is essential, numerous DER parts lie outside their immediate domain. As Figure 3 delineates, dissecting information from different sources - SCADA estimations, WAN organizations, brilliant meters, and inverters - at a headquarters and control focus is indispensable for recognizing expected dangers. Taking advantage of this rich information scene, as stressed by reports from [30,31,32] enables utilities to identify and safeguard against assaults focusing on their DER frameworks.

5.2. Response to Cyber Layer Attacks

Responding to cyberattacks on energy systems demands a nuanced approach tailored to the attack's nature and our confidence in its assessment. Depending on the severity and certainty, strategies can

range from dynamically adapting network architecture around suspicious devices (potentially using algorithms) to direct interventions like shutdowns, device deactivations, or manual task execution. Critically, core service systems must remain operational even during attacks, necessitating robust security and redundancy measures [33,34].

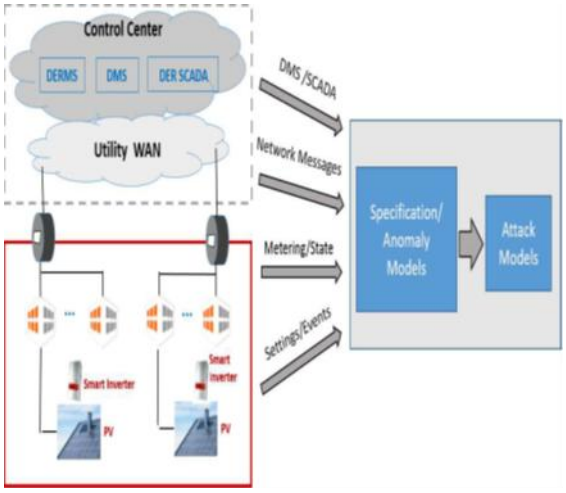

Figure 3. Detection of Cyber Layer Attacks [14].

6. Conclusion

Robust cybersecurity solutions are necessary to pave the way for extensive DER integration. This study proposes a dedicated research framework for DER cybersecurity in complex power systems, encompassing threat modeling, resilience analysis, and tailored prevention, detection, and response strategies across all system layers. By proactively addressing these challenges, this framework aims to secure a reliable and widespread DER integration into the modern power grid.

7. Future work

The analytics presented in this paper explore the fundamental problems of the proposed DER cyber security system. Advanced mathematics and statistical sciences can aid in solving these problems in the future because Cyber security has become increasingly complex, as it deals with integrated information systems and networks Accessing real-world data are necessary to understand these large and complex systems The proposed methodologies are based on validating experiments and models with mathematical ideas, focusing on the most widely used mathematical theories. These models can simulate the different properties of the systems studied by comparing them to the behavior of the existing system. However, the chosen mathematical approach is heuristic and depends on the researcher's background.

8. References

[1] S. H. et al., "Energy Web Chain: accelerating the energy transition with an open-source decentralized blockchain platform," Energy Web Foundation Publ., Oct. 2018. [Online]. Available: https://docslib.org/doc/10577118/the-energy-web-chain-accelerating-the-energy-transition-with-an-open-source-decentralized-blockchain-platform (accessed Apr. 27, 2024).

[2] I. MacGill, A. Bruce, and S. Young, "Renewable energy auctions versus green certificate schemes-lower prices but greater integration costs?," in Proc. IEEE PESGM, Aug. 2019. https://doi.org/10.1109/PESGM40551.2019.8973627

[3] A. Lee et al., "Cyber security for DER systems: National Electric Sector Cybersecurity Organization Resource (NESCOR)," 2013. [Online]. Available: https://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf (accessed May 01, 2024).

[4] "Federal renewable energy certificate guide," Office of Federal Sustainability, Council on Environmental Quality, 2016. [Online]. Available: https://www.sustainability.gov/pdfs/federal_rec_guide.pdf (accessed Mar. 01, 2024).

[5] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," Technol. Innov. Manag. Rev., vol. 4, no. 10, pp. 13-21, Oct. 2014. https://doi.org/10.22215/timreview/835

[6] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," Comput. Secur., vol. 77, pp. 262-276, Aug. 2018. https://doi.org/10.1016/j.cose.2018.03.011

[7] "NSA and CISA recommend immediate actions to reduce exposure across all operational technologies and control systems," Jul. 2020. [Online]. Available: https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF

[8] U. Cali, C. Lima, X. Li, and Y. Ogushi, "DLT/blockchain in transactive energy use cases segmentation and standardization framework," in Proc. IEEE PES Transactive Energy Syst. Conf. (TESC), Minneapolis, MN, USA, 2019, pp. 1-5. https://doi.org/10.1109/TESC.2019.8843372

[9] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653-659, Sep. 2017.

[10] T. Kenning, "Replication of cyberattacks on energy sector a threat to renewables," PV Tech, Sep. 07, 2018. [Online]. Available: https://www.pv-tech.org/news/replication-of-cyber-attacks-on-energy-sector-a-threat-to-renewables (accessed May 01, 2024).

[11] R. Kern, "Duke Energy hit by 650M cyber attempts to breach systems in 2017," Bloomberg Law News, 2018. [Online]. Available: https://news.bloomberglaw.com/environment-and-energy/duke-energy-hit-by-650m-cyber-attempts-to-breach-systems-in-2017 (accessed May 01, 2024).

[12] B. K. Sovacool, "Energy security: challenges and needs," Wiley Interdiscip. Rev. Energy Environ., vol. 1, no. 1, pp. 51-59, Jun. 2012. https://doi.org/10.1002/wene.13

[13] NESCOR, "Wide area monitoring, protection, and control systems (WAMPAC)-standards for cyber security requirements," 2012. [Online]. Available: http://smartgrid.epri.com/doc/ESRFSD.pdf

[14] J. Qi, A. Hahn, X. Liu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," IET Cyber-Phys. Syst., vol. 1, no. 1, pp. 28-39, Dec. 2016. https://doi.org/10.1049/iet-cps.2016.0018

[15] Ü. Cali and C. F. Lima, "Energy informatics using the distributed ledger technology and advanced data analytics," in Practice, Progress, and Proficiency in Sustainability, 2019, pp. 438-481. https://doi.org/10.4018/978-1-5225-8559-6.ch016

[16] E. K. Payne, Q. Wang, L. Shulin, and L. Wu, "Technical risk synthesis and mitigation strategies of distributed energy resources integration with wireless sensor networks and internet of things-review," J. Eng., vol. 2019, no. 18, pp. 4830-4835, Jun. 2019. https://doi.org/10.1049/joe.2018.9325

[17] U. Cali and A. Fifield, "Towards the decentralized revolution in energy systems using blockchain technology," Int. J. Smart Grid Clean Energy, vol. 8, no. 3, pp. 245-256, 2019. https://doi.org/10.12720/sgce.8.3.245-256

[18] "NISTIR 7628 guidelines for smart grid cyber security: vol. 3, supportive analyses and references," Smart Grid Interoperability Panel-Cyber Security Working Group, 2010. [Online]. Available: https://www.smartgrid.gov/files/documents/NISTIR_7628_Guidelines_for_Smart_Grid_Cyber_Security_Vol_3_201001.pdf (accessed Mar. 20, 2024).

[19] ENISA, "Distributed ledger technology & cybersecurity-improving information security in the financial sector," Jan. 18, 2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security

[20] S. Saxena, H. Farag, A. Brookson, H. Turesson, and H. Kim, "Design and field implementation of blockchain-based renewable energy trading in residential communities," in Proc. 2nd Int. Conf. Smart Grid Renew. Energy (SGRE), Nov. 2019. https://doi.org/10.1109/SGRE46976.2019.9020672

[21] W. Hua and H. Sun, "A blockchain-based peer-to-peer trading scheme coupling energy and carbon markets," in Proc. Int. Conf. Smart Energy Syst. Technol. (SEST), Sep. 2019. https://doi.org/10.1109/SEST.2019.8849111

[22] P. Xie et al., "Conceptual framework of blockchain-based electricity trading for neighborhood renewable energy," in Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integration (EI2), 2018. https://doi.org/10.1109/EI2.2018.8581887

[23] D. Livingston, V. Sivaram, M. Freeman, and M. Fiege, "Applying blockchain technology to electric power systems," JSTOR, 2018. [Online]. Available: https://www.jstor.org/stable/resrep21340

[24] M. Pipattanasomporn, S. Rahman, and M. Kuzlu, "Blockchain-based solar electricity exchange: conceptual architecture and laboratory setup," in Proc. IEEE ISGT, Feb. 2019. https://doi.org/10.1109/ISGT.2019.8791663

[25] E. B. Barker, "Guideline for using cryptographic standards in the federal government: cryptographic mechanisms," NIST Spec. Publ. 800-175B, Aug. 2016. https://doi.org/10.6028/NIST.SP.800-175B

[26] D. C. Smith, "Enhancing cybersecurity in the energy sector: a critical priority," J. Energy Nat. Resour. Law, vol. 36, no. 4, pp. 373-380, Sep. 2018. https://doi.org/10.1080/02646811.2018.1516362

[27] P. Bronski et al., "The decentralized autonomous area agent (D3A) market model," Energy Web, 2018. [Online]. Available: https://www.energyweb.org/insights/reports/

[28] A. Teymouri, A. Mehrizi-Sani, and C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," in Proc. IECON 2018-44th Annu. Conf. IEEE Ind. Electron. Soc., Oct. 2018. https://doi.org/10.1109/IECON.2018.8591583

[29] "How to recover from a cyber attack," IndustryWeek, Aug. 20, 2019. [Online]. Available: https://www.industryweek.com/sponsored/article/22028043/how-to-recover-from-a-cyber-attack

[30] U.S. Dept. Homeland Security, "Cybersecurity strategy," 2019. [Online]. Available: https://www.cybersecuritystrategydhs.gov/sites/default/files/publications/dhs-cybersecurity-fact-sheet.pdf (accessed Oct. 05, 2020).