Blockchain-Integrated Resilient Distributed Energy Resources Management System

Seerin Ahmad[1], Bohyun Ahn[1], Taesic Kim[1*], Jinchun Choi[1], Myungsuk Chae[2], Dongjun Han[2], Dongjun Won[2]

[1]Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX, 78363 USA
[2]Electrical and Computer Engineering, Inha University, Incheon, 22212 South Korea
seerin.ahmad@students.tamuk.edu, bohyun.ahn@students.tamuk.edu, taesic.kim@tamuk.edu, jinchun.choi@tamuk.edu, eric980206@inha.edu, hdj221124@inha.edu, djwon@inha.ac.kr

***Abstract*— Distributed energy resource management system (DERMS) is a supervision system managing distributed energy resources (DERs) in a distribution system. However, the centralized DERMS has a potential risk of a single point of failure posed by cyber-attacks (e.g., denial of service attacks and ransomware attacks). This will cause visibility and control losses of the DER system. In this paper, blockchain (BC) technology is leveraged to enhance the resilience of DERMS by recovering the operation of a DER system during the DERMS outage. The proposed BC system is a governance platform for the DER system proving security and resilient control services on behalf of the DERMS until the availability of the DERMS is recovered. The feasibility of the proposed BC-integrated DERMS system toward a resilient DER system is validated by using a cyber-physical co-simulation testbed.**

Keywords—blockchain, co-simulation, cybersecurity, distributed energy resource (DER), distributed energy resources management system (DERMS)

I. INTRODUCTION

Current electric power grid is undergoing transition to the increasing penetration of distributed energy resources (DERs) such as photovoltaic (PV) system, energy storage systems (ESSs), wind turbine (WT) systems, electric vehicle (EV) and controllable loads in distribution systems [1]. Broadly dispersed DERs, with advanced communication and computing systems, are expected to improve the power grid resilience if these smart DER capabilities are secured and coordinated with remote power system management systems such as a DER management system (DERMS) [2] and a DER aggregator for managing small DER devices [3]. Moreover, IEEE 1547-2018 [4] mandates advanced DER functions for grid services such as voltage regulation and ride-through using the DERMSs and/or DER aggregators in an effort of standardization for interconnection of DERs to the grid.

A DERMS is a mostly utility-owned command and control (C2) platform that remotely coordinates a group of DERs in a power distribution system by monitoring DER assets, forecasting, and optimizing operation of the DER system [5]-[8]. Austin Energy's Sustainable and Holistic Integration of Energy Storage and Solar Photovoltaics project [9] are examples of DERMSs operated by utilities. Typically, the DERMS is a central controller implemented in a utility server or cloud that receives real-time grid data from advanced metering infrastructure (AMI) (e.g., smart meters) and DER system data from DER smart inverters and then sends control commands to the DER inverters and controllable switches [10], [11]. However, the centralized DERM system is vulnerable to a single point of failure. Especially, cyberattacks targeting the centralized DERMS is a significant threat to the DER system and may lead to severe disturbance of DER-rich power grid as well [12], [13].

First cyberattack on U.S. grid (sPower) was reported on Mar. 5, 2019 [14]. A denial of service (DoS) attack disabled Cisco Adaptive Security Appliance (ASA) devices ringing power grid control systems in Utah, Wyoming and California. The grid operators were temporarily blinded to wind and solar DER sites totaling 500 Megawatts (i.e., SCADA visibility loss). This real incident using DOS attack shows the significance of securing grid control systems such as DERMSs. Furthermore, malware attacks such as ransomware attacks have recently targeted industrial control systems (ICS) and increased about 500% from 2018 to 2020 [15]. It is anticipated that more ransomware attackers will also target smart grids such as substations and DER systems [16]. The ransomware attacks encrypt the important files (i.e., denial-of-resource) in a DERMS, leading to a loss of availability of the DER system. Only payment of the ransom of the infected systems can be recovered. Therefore, it is imminent to develop cyber-resilient DERMS mitigating cyber-attacks causing a single point of failure.

Extensive studies have been done to address cybersecurity challenges in the DER systems. Overall, network-based security defense techniques [17]-[20] have been mostly proposed such as cryptography, public key infrastructure (PKI), moving target defense, and software-defined network (SDN) for a resilient DER network. Besides, real-time intrusion detection systems (IDSs, mostly false data injection attacks) have been widely studied using artificial intelligence and/or model-based methods [21]-[23]. In [23], a malicious DERMS controller that sends falsified control commands to DER inverters is detected by a de-centralized detection method using multivariate linear regression algorithm in DER inverters. Furthermore, attack resilience is considered for cyber, physical device, and utility layer security measures at multiple levels of DER for different attack classes to ensure that the grid can remain operational during an attack [24]. However, mitigating attacks causing a single point of failure of the DERMS has been less studied.

Blockchain (BC) is a distributed ledger that maintains a continuously growing list of data records secured from tampering and revision by using cryptography, public key PKI, consensus, and access control technologies [25]. The emergence of blockchain technology incorporating smart contracts has been applied to DER systems or smart grids [26]-[32]. BC technology has been used for secure energy trading [26], [27], access control [28], secure supply chain

This research was supported by the Department of Energy (DoE) under award No. DE-EE0009026, the National Science Foundation (NSF) under award No. CNS-2219733 and the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20214000000820).

978-1-6654-3254-2/22/$31.00 ©2022 IEEE

[29], man-in-the-middle (MitM) attack detection [30], DER firmware update [31], and inverter control [32]. In an effort of standardization, IEEE Blockchain Technical Committee suggested the basic framework and principles of IEEE Blockchain-enabled Transactive Energy (BCTE) for using BC technology in power and energy domains [33]. Therefore, it is expected that BC systems will be part of the modernized power grid by leveraging broader participation in the DER market, security, and resilience of power grid. However, the practical investigation of mitigating the threat of a single point of failure of the DERMS using BC technology has not been studied to the authors' best knowledge.

This paper introduces a potential vulnerability of a single point of failure of the centralized DERMS by cyber-attacks and proposes a BC-integrated resilient DERMS framework. A multichannel BC governance system is designed to build a cooperative security ecosystem in a multiple stakeholder-involved DER system where DER devices are blockchain client nodes and participating multiparty are blockchain clients. Therefore, BC system enables to securely share DER system and grid data among clients and provides control commands to DER device when the DERMS is failed or compromised by cyber-attacks. The concept of the proposed BC-integrated resilient DERMS is validated by a case study of voltage recovery control during the DERMS outage caused by DOS attack using a cyber-physical co-simulation testbed built-in MATLAB/Simulink in a PC interfacing with a Hyperledger-Fabric BC platform implemented in a PC.

II. Case Studies of Cyber-Attack Targeting DERMS

A. DERMS

Fig. 1 shows an example of DERMS-to-DER communication architecture [34]. IEEE 2030.5 network protocol is applied for communications between the utility DERMS and DER systems through connections via DER facility controller, an aggregator, or direct connections. In the direct DER communications, either the smart inverter control unit (SMCU) or a separate gateway/control unit is the IEEE 2030.5 client. The DER aggregator coordinates small DERs as an IEEE 2030.5 server and communicates with the DERMS as a client. The general roles of a DERMS are available in [35].

B. Two Cases of Cyber-Attacks

Fig. 1 illustrates two attack cases that target the operational failure of a DERMS, consequently causing the significant loss of visibility and controllability of the DERs and potentially disrupting the local power grid: 1) (Distributed) DOS ((D)DOS) attack and 2) ransomware attack.

A DOS attack occurred at an electric utility on March 5, 2019, which left grid operators temporarily blinded to generation sites including DERs for more than 10 hours [14]. Such a DOS attack is possible if an adversary finds the firewall(s) of a DERMS exposed online via specialized device IP and port search tools (e.g., Shodan). Then, the flood of fake requests disables the network devices of the DERMS (e.g., Cisco ASA that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities) using DOS attack tools (e.g., Slowloris). Moreover, DDOS will directly target the DERMS server with numerous bots. Recovery time of DOS may take several hours to a day [14].

The other potential threat is ransomware attacks. In April 2022, three Germany-based wind-energy companies were targeted by the Conti ransomware group and then prompted to shut down remote-control systems for roughly 2,000 wind turbines for about a day [35]. A similar case might happen in DERMS. For example, a ransomware actor purchases a stolen credential from legitimate insiders, cybercrime partners, or third-party intrusion brokers as initial access to a DERMS server. Upon obtaining privileged access, the actor can establish a persistent backdoor platform in the server to upload ransomware and export sensitive data [16]. The adversary remotely encrypts the critical files for DERMS monitoring and control and then starts to demand a significant ransom payment to restore the locked/compromised DERMS. In addition, the exfiltrated data can be exploited to require a more ransom payment, threatening victim employees with an

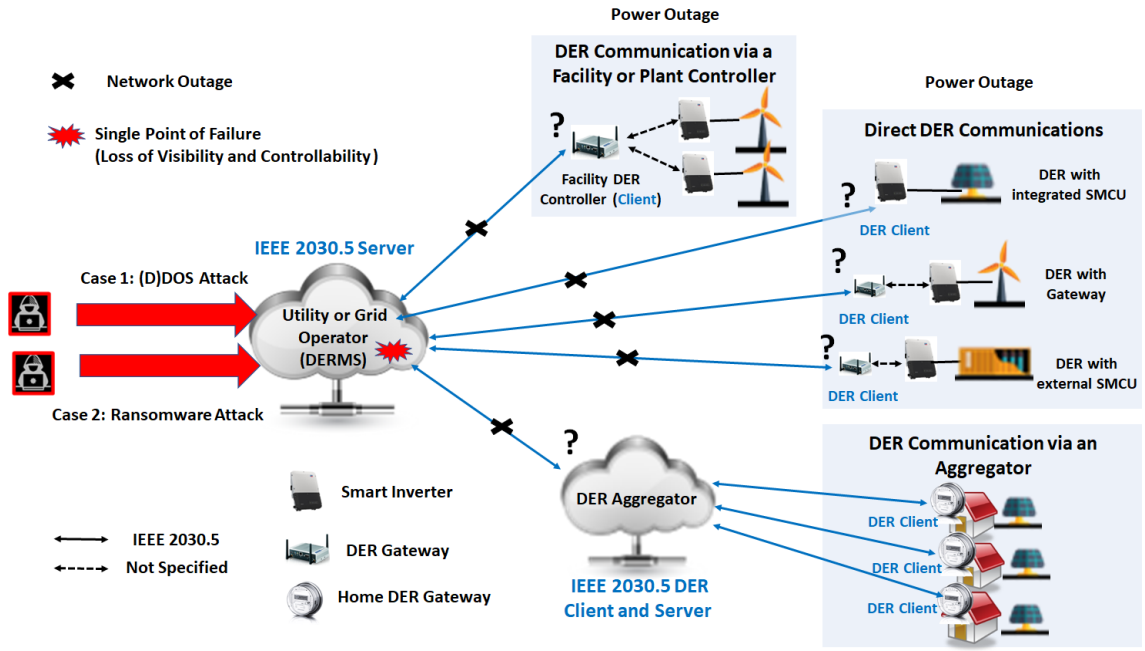


Fig. 1. Cases of cyber-attacks targeting a DERMS in a DER system.

auction or release to the public through an email network. Recovery time from a ransomware attack is dependent on the time of DERMS operator pays a ransom. However, additional recovery time will be required to fully investigate the impacts of malware and data breach.

III. Proposed Method

This paper proposes a BC-integrated DERMS framework enabling to operate the DER system to continue to function correctly despite the failure of the DERMS caused by cyberattacks. This section introduces the concept of BC-based cooperative cyber-resilient ecosystem for multipart-involved DER systems, an overall recovery process, and the proposed smart-contract defined DERMS control.

A. BC-Based Cooperative Cyber-Resilient Ecosystem

Fig. 2 illustrates the concept of BC-based cooperative cyber-resilient ecosystem. For a multiparty environment, standardizing the mutual agreement procedure in BC will support multiple stakeholders moving toward a common set of effective cyber-resilient grid practices. The proposed BC-based security governance platform will build a collaborative security ecosystem where multiparty can seamlessly handle the utility-, aggregator-, or vendor-identified incidents through effective notification, coordination, disclosure, and validation mechanism. In this way, the multiparty will have enhanced visibility into the methods, applications, and services to ensure integrity and authenticity of all security critical assets (e.g., software/firmware) provided by the vendors, thus providing a viable way to manage the evolving cyber risks on the DER systems. By participating the BC network, each party can share security responsibility for achieving security and grid resilience. Parties at the same channel can share and manage data sources in the channel. Off-chain is available to store their confidential data and publish hash of that data into the ledger. Therefore, data privacy will be improved in a shared platform. All governance functions are programmed in the form of smart contracts with mutual agreement of parties related to the functions. This paper assumes that the BC system already exists and focuses on the use of the control channel for recovering a DER system when a DERMS is out of service due to the cyber-attacks.

B. BC-Integrated DERMS

Fig. 3 shows the proposed BC-integrated DERMS controlled by DERMS smart contract and an overall recovery process of the malfunctioned DERMS by DOS or ransomware attacks. In the BC-integrated DERMS, the blockchain peers/nodes are used as a secure medium to deliver critical information among DER inverters through the distributed ledgers for secure and resilient control purpose as well as authorized stakeholders for better situational awareness. Connected to the blockchain nodes, DERs send their local measurements to the BC system such as voltage, current, and power and can access the shared DER data and control commands. Such monitoring and controlling DERs are managed by the DERMS control smart contract.

Once an IDS detects the malfunctioned DERMS, the DERMS smart contract is activated. Based on the measurement data stored in the ledger and tertiary control requirement by the distribution system operator (DSO), DERMS smart contract generates control commands for the DER inverters acting as a virtual DERMS. The shared data and control commands written in the ledgers are then available to the DER inverters. Therefore, the BC network provides an alternative channel to the DER system on behalf of the DERMS, enabling cyber-resilient operations for the DER system such as adaptive frequency-watt control and volt-var control depending on the grid condition. The DERMS smart contract will be deactivated once the DERMS is recovered. Moreover, an incentive mechanism that provides credits to the peers will be activated, which, however, is not considered in this paper.

C. Smart Contract-Defined DERMS Control

As an example of smart contact-defined DERMS control, this paper shows a voltage restoration control at point-of-coupling (PCC) of a DER system. The testing DER system in IEEE 13 Node Test Feeder circuit consists of multiple smart

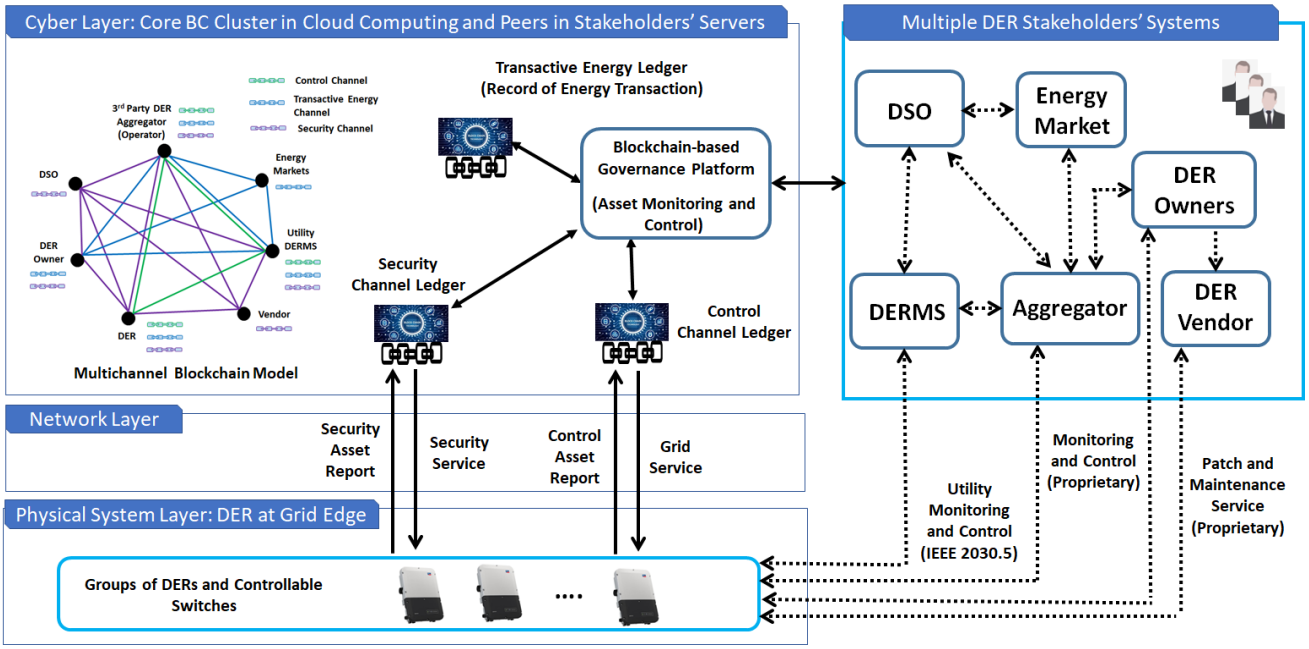


Fig. 2. Concept of blockchain-based cooperative cyber-resilient ecosystem for multiparty-involved DER systems.

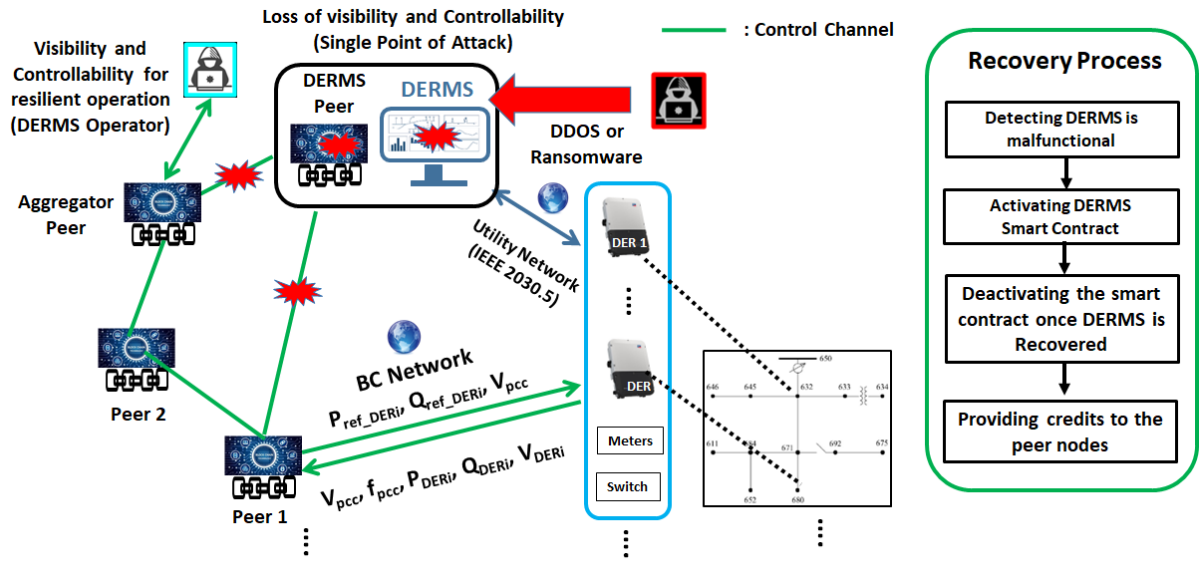


Fig. 3. Proposed blockchain-integrated DERMS controlled by DERMS Control Smart Contract and an overall recovery process of the malfunctional DERMS by DOS or ransomware attacks.

inverters, a swing bus, a wind WT, a PV, an ESS, loads and a DERMS implemented in a cloud server [34].

Owing to the page limit, this paper only shows the ESS inverter control (i.e., *DER1*) and the ESS-based voltage restoration. Fig. 4 illustrates the ESS inverter control model. The primary controller controls the voltage, current, active, and reactive power flow of the ESS inverter. A droop control is applied for primary control of the controller. Combination of active/reactive (P/Q) power calculation and droop control determines $I_{edq0,ref}$ (= $I_{ed,ref}$ and $I_{eq,ref}$) which can be expressed as follows:

$$I_{ed,ref} = \frac{2}{3}\frac{P_{eref}}{V_{ed}} \tag{1}$$

$$I_{eq,ref} = -\frac{2}{3}\frac{Q_{eref}}{V_{ed}} \tag{2}$$

where P_{eref} and Q_{eref} are the active and reactive power references, respectively; and V_{ed} is the measured line voltage. Through the P/Q calculation and droop control, P_{eref} and Q_{eref} are computed as follows:

$$P_{eref} = P_{ref\_DER1} + \Delta P_{edroop} \tag{3}$$

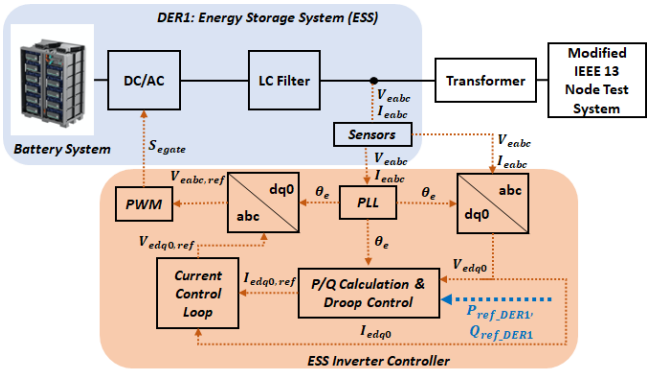


Fig. 4. Detailed ESS control model in IEEE 13 node test feeder circuit.

$$Q_{eref} = Q_{ref\_DER1} + \Delta Q_{edroop} \tag{4}$$

$$\Delta P_{edroop} = -\frac{f - f_0}{K_{eP}} \tag{5}$$

$$\Delta Q_{edroop} = -\frac{V - V_0}{K_{eQ}} \tag{6}$$

where P_{ref_DER1} and Q_{ref_DER1} are active and reactive power control commands from the BC-enabled DERMS, respectively; ΔP_{edroop} and ΔQ_{edroop} denote the variations of P and Q, respectively; f_0 and V_0 are nominal frequency and voltage of the system; f and V are measured inverter output

```
/// UpdateAsset updates the assets information of asset with
given parameters in world state
func (s *SmartContract) UpdateAsset(ctx
contractapi.TransactionContextInterface, id string, V_pcc
float64, f_pcc float64, V_DER1 float64, P_DER1 float64,
Q_DER1 float64, V_DER2 float64, P_DER2 float64, Q_DER2
float64, V_DER3 float64, P_DER3 float64, Q_DER3 float64,
V_DER4 float64, P_DER4 float64, Q_DER4 float64) (*Asset,
error) {
        // first checking the existance of the asset ID in
the ledger.
        exists, err := s.AssetExists(ctx, id)
        if err != nil {
                // return nil, err
                return nil, err
        }
        if !exists {
                // return nil, fmt.Errorf("the asset %s does
not exist", id)
                return nil, fmt.Errorf("the asset %s does
not exist", id)
        }
        chkasset, err := s.QueryAsset(ctx, id) // calling
QueryAllAssets function to get full range of asset
information
        if err != nil {
                // return nil, err
                return nil, err
        }
        // overwritting original asset with new asset
        asset:= Asset{
                ID:              id,
                Vsys:            V_pcc,
                Fsys:            f_pcc,
                Vder1:           V_DER1,
                Pder1:           P_DER1,
                Qder1:           Q_DER1,
                Vder2:           V_DER2,
                Pder2:           P_DER2,
                Qder2:           Q_DER2,
                Vder3:           V_DER3,
                Pder3:           P_DER3,
                Qder3:           Q_DER3,
                Vder4:           V_DER4,
                Pder4:           P_DER4,
                Qder4:           Q_DER4,
        }
```

Fig. 5. A sample of smart contract (chain code written in Golang) for the DER system monitoring.

frequency and voltage, respectively; and K_{eP} and K_{eQ} are droop coefficients.

The DERMS smart contract consists of two parts: 1) Monitoring script that describes a rule of data collection and sharing between the blockchain network and DER inverters and authorized multiparty clients (e.g., DERMS operator and DER owners) and 2) Control script that is a logic statement for voltage recovery at PCC in the DER system managed by the DERMS. Monitoring script stores DER system data in the ledger including *V_pcc, f_pcc, P_DERi, Q_DERi, V_DERi* as shown in Fig. 3 ($1 \leq i \leq n$). Therefore, the DERMS operators still monitor the status of the DER system by reading the ledger data. Control script generates new P_{ref_DER1} and Q_{ref_DER1} based on and stores them in the ledger. Then, each DER can read the updated reference values in the ledger (World State in Hyperledger Fabric). Fig. 5 shows the smart-contract for BC-enabled DERMS in the blockchain network in Golang.

IV. VALIDATION

Fig. 6 shows the experimental setup to validate the concept of the proposed BC-integrated DERMS framework using two computers with an Intel® Core™ i5-2410M CPU @2.30GHz, 64-bit OS as PC-1 where the physical DER system model [34] is implemented in MATLAB/Simulink and Intel® Core™ i5-8250U CPU @3.4GHz, 64-bit OS as PC-2 for the BC server and the DERMS. The BC server is designed using Hyperledger-Fabric platform [37]. A MATLAB function block [32] is used to establish a network interface between the Simulink model and the BC/DERMS server using local Wi-Fi. The system bus frequency is 60 Hz (i.e., *f_pcc*), and the nominal voltage is 4.16 kV (i.e., *V_pcc*). The rated power of WT, PV are 2 MVA and 1MW, respectively. The ESS capacity is 1 MWh, and the resistive, inductive, and capacitive loads are evenly connected to the other buses, where the real power demand of the distribution system is 3.5 MW; the reactive power demand of inductive loads is 2.102 MVAR; and the reactive power demand of capacitive loads is 0.7 MVAR. The sampling times of the primary control and DERMS control are 50 ms and 1 s, respectively.

Fig. 7 depicts a screenshot of the ledger data showing monitoring the status of the DER system. The monitoring data includes *V_pcc, f_pcc, V_DERi, P_DERi, Q_DERi, V_DERi, P_DER4, Q_DER4*, where *i* represents the number of DER ($1 \leq i \leq 4$). The integrity-guaranteed DER system data can be shared with authorized BC clients including a DERMS operator. Therefore, continuous situational awareness of the DER system is possible although the main DERMS lost visibility by the cyber-attacks.

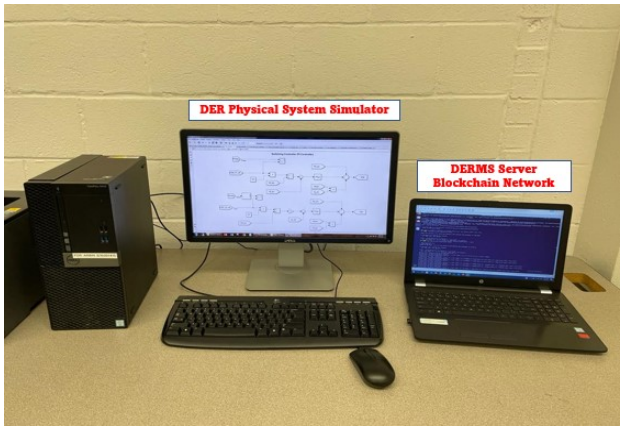


Fig. 6. Experimental setup of co-simulation.

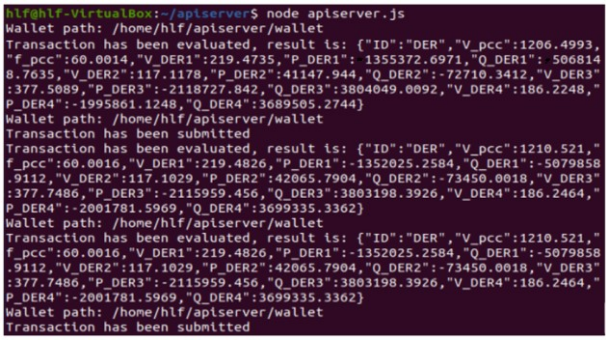
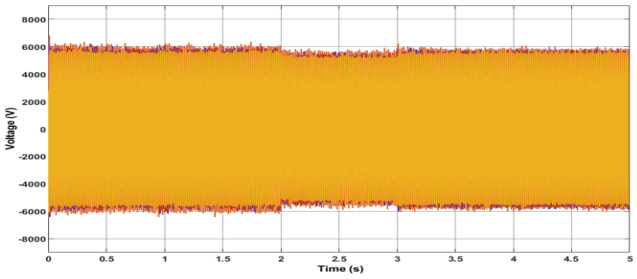
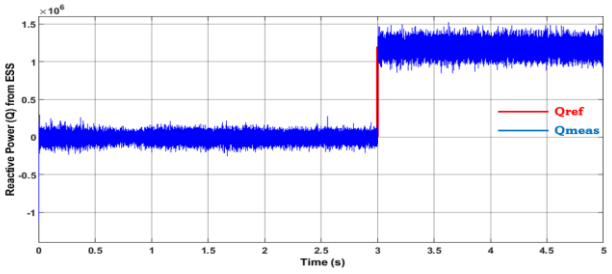


Fig. 7. Screenshot of PCC voltage and frequency and DER device data in the blockchain ledger (World State).

Fig. 8 shows a voltage recovery control by the smart contract defined DERMS control when an inductive load is significantly increased after 2 s. Fig 8(a) shows the voltage sag at PCC caused by increased inductive load after 2 s. The smart contract computes and stores *Qref_DER1* in the ledger which is available to *DER1* (i.e., ESS) around 3 s. Using the new *Qref_DER1*, *DER1* recovers the voltage at PCC. Therefore, the PCC voltage returns to the original value. Fig 8(b) shows the measured reactive power from the *DER1* (shown in blue) to recover the voltage at PCC which fully follows the reference set value (shown in red). However, the DER system will operate in unstable conditions or needs to be shut down if a conventional central DERMS is out of control by cyber-attacks. It is obvious that by integrating the BC system, resiliency of the DERMS has been significantly improved.



(a)



(b)

Fig. 8. Experimental results: (a) voltage waveform and (b) ESS control.

V. CONCLUSION

This paper introduces two attack scenarios targeting a single point of failure of conventional DERMS based on real-world incident cases and threat modeling approaches. Furthermore, this paper briefly describes an overview of BC-based governance model for DER systems. Finally, a BC-integrated resilient DERMS framework has been proposed to

mitigate the cyber-attacks targeting the DERMS by substituting the operation of a DER system during the DERMS outage. The proposed method is validated by a case study of voltage recovery at PCC using a cyber-physical co-simulation testbed. Future works include: 1) designing a hardware-in-the-loop testbed, 2) adding more DERM control and intrusion detection logic in smart contracts and 3) finally developing the blockchain-based cooperative cyber-resilient ecosystem for multiparty-involved DER systems.

REFERENCES

[1] B. Kroposki, et al., "Achieving a 100% renewable grid: Operating electric power energy systems with extremely high levels of variable renewable," *IEEE Power and Energy Magazine*, vol. 15, no. 2, pp. 61-73, 2017.

[2] N. Bilakanti, N. Gurung, H. Chen, and S. R. Kothandaraman, "Priority-based management algorithm in distributed energy resource management systems," in *Proc. 2021 IEEE Green Technologies Conference (GreenTech)*, Apri. 7-9, 2021, pp. 351-356.

[3] M. Obi, T. Slay, and R. Bass, "Distributed energy resources aggregation using customer-owned equipment: A review of literature and standards," *Energy Reports*, vol. 6, pp. 2358-2369, Nov. 2020.

[4] IEEE, "IEEE Std. 1547-2018—IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," 2018.

[5] J. Wang, J. S. Jing, R. Yang, B. Palmintier, S. Tiwari, and Y. Zhang, "Hardware-in-the-loop evaluation of an advanced distributed energy resource management algorithm," in *Proc. 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, D.C., USA, Feb. 17-20, pp. 1-5.

[6] L. Strezoski, I. Stefani, and B. Brbaklic, "Active management of distribution systems with high penetration of distributed energy resources," in *Proc. IEEE EUROCON 2019 -18th International Conference on Smart Technologies*, Novi Sad, Serbia, Jul. 1-4, 2019, pp. 1-5.

[7] IEEE Std. P2030.11-2021: 'IEEE guide for distributed energy resources management systems (DERMS) functional Specification,' *IEEE*, Jun. 2021.

[8] B. Seal, A. Renjit, and B. Deaver, "Understanding DERMS," CA: *Electric Power Research Institute*, Jul. 13, 2018.

[9] Austin Energy, "Distributed energy resource (DER) strategy, next steps, and preliminary findings from austin SHINES DER integration project," White Paper, Dec. 2021.

[10] L. Strezoski, I. Stefani, and B. Brbaklic, "Active management of distribution systems with high penetration of distributed energy resources," in *Proc. IEEE EUROCON International Conference on Smart Technologies*, Novi Sad, Serbia, July 1-4, 2019, pp. 1-5.

[11] AutoGrid DERMSTM, "The industry's most comprehensive application for managing DERs," [Online]. Available: https://www.auto-grid.com/

[12] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," Sandia National Laboratories, Technical Report, 2017.

[13] B. Ahn, T. Kim, J. Choi, K. Park, and D. Won, "A cyber kill chain model for distributed energy resources (DER) aggregation systems," in *Proc. 2021 IEEE PES Innovative Smart Grid Technologies Conference North America*, Washington, DC, USA, Feb. 16-18, 2021, pp. 1-5.

[14] 'Denial of service condition' disrupted US energy company operations. [Online]. Available: https://techcrunch.com/2019/05/02/ddos-attack-california-energy/

[15] S. Larson and C. Singleton, "Singleton, ransomware in ICS environments," White Paper, Dragos, Inc., Dec. 2020.

[16] Y. Su, B. Ahn, S. Alvee, T. Kim, J. Choi, and S. Smith, "Ransomware security threat modeling for photovoltaic systems, in *Proc. 2021 6th "IEEE Workshop on Electronic Grid (eGrid)*, New Orleans, LA, Nov. 8-10, 2021, pp.1-5.

[17] J. Henry, et al., "Cyber security requirements and recommendations for CSI RD&D Solicitation #4 distributed energy resource communications," Oct 2015.

[18] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Technical Report, SAND2017-13262, Dec. 2017.

[19] D. Saleem and C. Carter, "Certification procedures for data and communications security of distributed resources, NREL Technical Report, July 2019.

[20] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment, *IET Cyber Physical System*, vol. 5, no. 3, pp. 274–282, Mar. 2020.

[21] J. Appiah-Kubi and C. C. Liu, "Decentralized intrusion prevention (DIP) against coordinated cyberattacks on distribution automation systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 389–402, Oct. 2020.

[22] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, "Countering FDI attacks on DERs coordinated control system using FMI-compatible cosimulation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1640–1650, Mar. 2021.

[23] A. K. Jain, N. Sahani, and C. C. Liu, "Detection of falsified commands on a DER management system, *IEEE Trans. Smart Grid*, vol. 13, no. 2, p. 1322-1334, Mar. 2022.

[24] J. Qi, A. Hahn, X. Lu, J. Wang, and C-C. Liu, "Cybersecurity for distributed energy resource and smart inverters," *IET Cyber-Phys, Syst., Theory Appl*., vol. 1, no. 1, pp. 28-39, Dec. 2016.

[25] N. Prusty, Building Blockchain projects, Packt Publishing, Feb. 2017. 20. Microgrid Media, "It's like the early days of the internet, Blockchain-based microgrid tests P2P energy trading in Brooklyn," Mar. 2016.

[26] American Public Power Association, "Blockchain REC trading platform set to launch in the U.S.," [Online]. Available: https://www.publicpower.org/periodical/article/blockchain-rec-trading-platform-set-launch-us

[27] T. Gaybullaev, H-Y. Kwon, T. Kim, and M-K. Lee, "Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption," *Sensors*, vol. 21. no. 6, 2024, Mar. 2021.

[28] Y. Ding, "SC-RBAC: A smart contract based RBAC Model for DApps.," in *Proc. International Conference on Human Centered Computing*. Springer, Cham, 2019.

[29] M. Mylrea, and S. N, G. Gourisetti, "Blockchain: Next generation supply chain security for energy infrastructure and NERC critical infrastructure protection (CIP) compliance," *Journal on Systemics, Cybernetics and Informatics*, vol. 16, no. 6, pp. 22-30, Nov. 2018.

[30] J. Choi, B. Ahn, G. Bere, S. Ahmad, A. Mantooth, and T. Kim, "Blockchain-based man-in-the-middle (MITM) attack detection for photovoltaic systems," in *Proc. 2021 IEEE Design Methodologies for Power Electronics*, Bath, UK, Jul. 14-15, 2021, pp. 1-6.

[31] J. Choi, B. Ahn, S. Pedavalli, S. Ahmad, A. Villasenor, and T. Kim, "Secure firmware update and device authentication for smart inverter using blockchain and physically unclonable function (PUF)-embedded security module," in *Proc. 2021 6th IEEE Workshop on Electronic Grid (eGrid)*, New Orleans, LA, Nov. 8-10, 2021, pp.1-4.

[32] A. A. Hadi, G. Bere, B. Ahn, and T. Kim, "Smart contract-defined control and co-simulation for smart inverters in a photovoltaic (PV) system and blockchain network," in *Proc. 2020 IEEE CyberPELS Workshop*, Oct. 13, 2020, pp.1-6.

[33] F. Rahimi et al., "Blockchain transactive energy (BCTE) position paper," *IEEE Position & Vision Statement Paper*, May 2021

[34] J. Kim, K. Park, B. Ahn, J. Choi, Y. Noh, D. Won, and T. Kim, "Real-time hardware-in-the-loop distributed energy resources system testbed using IEEE 2030.5 standard," in *Proc. 2021 IEEE PES Innovative Smart Grid Technologies – Asia (ISGT Asia*), Brisbane, Australia, Dec. 5-8, 2021, pp. 1-5.

[35] B. Seal, and R. Uluski, "Integrating smart distributed energy resources with distribution management systems," The Electric Power Research Institute (EPRI), 2012.

[36] Wind-energy sector hit in wave of hacks. [Online]. Available: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000

[37] Hyperledger Fabric – Hyperledger Foundation. [Online]. Available: https://www.hyperledger.org/use/fabric