IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 November 2024, accepted 7 December 2024, date of publication 12 December 2024, date of current version 26 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3516581

RESEARCH ARTICLE

Blockchain-Assisted Resilient Control for Distributed Energy Resource Management Systems

SEERIN AHMAD[1], (Graduate Student Member, IEEE), KALYAN NAKKA[2], TAESIC KIM[3], (Senior Member, IEEE), DONGJUN HAN[4], (Graduate Student Member, IEEE), DONGJUN WON[4], (Senior Member, IEEE), AND BOHYUN AHN[3], (Member, IEEE)

[1]Department of Electrical Engineering and Computer Science, Texas A&M University–Kingsville, Kingsville, TX 78363, USA
[2]Department of Computer Science and Engineering, Texas A&M University, College Station, TX 77843, USA
[3]Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO 65211, USA
[4]Department of Electrical and Computer Engineering, Inha University, Incheon 22212, South Korea

Corresponding author: Taesic Kim (tkx96@missouri.edu)

This work was supported in part by the Department of Energy (DoE) under Award DE-EE0009026, and in part by the National Science Foundation (NSF) under Award CNS-2219733.

ABSTRACT Grid resilience has become a paramount concern in today's dynamic energy landscape, wherein the mass integration of distributed energy resources (DERs) plays a crucial role in achieving flexible and resilient power grids. A DER management system (DERMS) is a remote monitoring and control system managing DERs in a distribution system, which is becoming increasingly important for a DER-rich power grid. However, an outstanding issue is a single point of failure of the centralized DERMS by cyberattacks, which threatens grid stability and results in regional power outages in the worst case. This paper proposes a novel approach to address the resilience challenges faced in the centralized DERMS through the development of a blockchain (BC)-assisted resilient control mechanism. The main idea is to create a virtual DERMS monitoring and control using BC smart contract and network that takes over seamlessly in the event of a failure of the DERMS. This BC system enables securely sharing DER and grid data among BC clients and provides control commands to DERs when the DERMS is a denial-of-service condition. To demonstrate the effectiveness of the proposed BC-assisted DERMS, voltage and frequency control recovery cases are tested in a real-time hardware-in-the-loop DER system testbed.

INDEX TERMS Blockchain, cybersecurity, distributed energy resource, distributed energy resource management system, grid resilience.

I. INTRODUCTION

Current electric power grid is undergoing transition to clean energy using distributed energy resources (DERs) such as photovoltaic (PV) systems, energy storage systems (ESSs), wind turbine (WT) systems, electric vehicle charging systems (EVCSs) and controllable loads in distribution systems and subtransmission systems [1]. Broadly installed 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 DER management systems (DERMS) [2] and DER aggregators managing groups of small DER devices in residential area [3]. Besides, IEEE 1547-2018 [4] mandates DERs provide grid-supportive functions such as voltage regulation and ride-through by using the DERMS in an effort of standardization for interconnection of DERs to the power grid.

A DERMS is a command and control (C2) platform that remotely coordinates a group of DERs in a power distribution system by monitoring DER assets, forecasting, and

The associate editor coordinating the review of this manuscript and approving it for publication was Yifan Zhou.

optimizing operation of the grid-connected DERs [5], [6], [7], [8], [9]. Typically, the DERMS is implemented in a utility server or a cloud platform that receives real-time grid data from advanced metering infrastructure (AMI) (e.g., smart meters) and DER system data from DERs and then sends control commands to the DER inverters and controllable switches [6], [10] while interacting with DER service requesting entities (e.g., distribution management system (DMS)). However, the current centralized DERMS is vulnerable to a single point of failure. Especially, cyberattacks targeting the DERMS will be a significant threat to the DER operators and may lead to severe disturbance of DER-rich power grid as well [11], [12].

The first cyberattack on U.S. power grid took place on a Utah-based renewable energy generation provider (sPower) on Mar. 5, 2019 [13]. This attack (i.e., firewall firmware attack) disabled Cisco Adaptive Security Appliance (ASA) devices by unexpected continuous reboots of the devices. This incident leveraged a denial of service (DOS) condition between the control center and the DER sites, resulting in 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. This real incident demonstrates the significance of securing grid control systems such as DERMS. Furthermore, malware attacks (e.g., ransomware attacks) have recently targeted industrial control systems (ICS) and increased about 500% from 2018 to 2020 [14]. It is anticipated that more ransomware attackers will also target smart grids such as substations and DER systems [15]. The successful ransomware attacks can lock the important files (i.e., denial-of-resource) in a DERMS, leading to a loss of availability of the DER system. Therefore, it is imminent to develop solutions to improve cyber-resilience of DERMS to ensure the reliable and secure operation of power grid.

Numerous research has been conducted to address emerging DER cybersecurity threats. First of all, network-based security defense techniques [16], [17], [18], [19] have been widely proposed such as encryption, public key infrastructure (PKI), moving target defense, and software-defined network (SDN) for a resilient DER network. Besides, real-time intrusion detection systems (IDS) have been studied using artificial intelligence (AI) and/or model-based methods [20], [21], [22]. In [22], cyberattack models aimed at compromising DERMS are proposed through the falsification of control commands and alteration of algorithms. Additionally, decentralized intrusion detection methods for inverters, utilizing multivariate linear regression, are suggested as essential tools for countering attacks. The authors in [21] evaluate the resilience of a PV-based DER system against false data injection (FDI) attacks and introduces a neural network-based algorithm for detecting and mitigating the FDI attacks. In [23], a rule-based fallback control strategy is proposed for the ESS in an islanded microgrid to enhance microgrid resiliency against DOS attacks. In [24], a hybrid IDS approach using both physical and cyber network data in DER systems is proposed to achieve robust identification and mitigation of malicious events on the DER system. Furthermore, a multi-level attack resilience framework has been proposed for cyber-physical device, and utility layer of a DER system against different attack classes to ensure that the grid still remains operational under the cyberattacks [25]. However, mitigating attacks causing a single point of failure of the DERMS has been less studied.

BC system is a multiple peer network which shares distributed ledgers that maintain data records secured from tampering and revision by using cryptography and consensus and access control through smart contracts [26]. The emergence of BC technology incorporating smart contracts has been applied to DER systems or smart grids [27], [28], [29], [30], [31], [32], [33]. BC technology has been used for secure energy trading [27], [28], DER access control [29], secure supply chain [30], man-in-the-middle (MITM) attack detection [31], DER device firmware update [32], and inverter control [33], [34]. In an effort of standardization, IEEE BC Technical Committee suggested the basic framework and principles of IEEE BC-enabled Transactive Energy (BCTE) for using BC technology in power and energy domains [35]. SunSpec BC Work Group developed a BC-based key registry for DER devices which can provide an accessible repository for querying security-critical information about DER devices and their keys with high availability and strong integrity protection of the stored information [34]. 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, 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.

There have been recent studies addressing the management and control of DERs using DERMS. Reference [36] discusses the performance evaluation of a new DERMS algorithm which includes predictive state estimation (PSE) and online multiple objective optimization (OMOO) to dispatch the legacy devices and DERs. In [37], the authors implemented a scalable and fast optimal power flow (OPF) algorithm integrated with a state estimation solver for DERMS to control a large distribution network of high DER penetration with fast DERs dispatching every 4 seconds. The author in [38] developed a DERMS to address voltage regulation that uses optimization algorithms such as Real-Time Optimal Power Flow (RTOPF) algorithm. DERMS automatically solves overloads, overvoltage, undervoltage, reverse power flows, as well as miscoordination of the protective devices in real time in [6]. However, resilience that is the ability to withstand and recover from deliberate attacks and accidents to the current centralized DERMS should be further studied.

The authors proposed a new concept of BC-integrated resilient DERMS [39] where a BC system enables to share DER data and control commands through the BC ledgers.

The concept of the BC-integrated resilient DERMS was validated by a simple case study of voltage recovery control during a DERMS outage in a non co-simulation testbed environment using MATLAB/Simulink in a PC interfacing with a Hyperledger Fabric (HLF) BC server. This paper is an extended work of [39] to develop a real-time BC-assisted resilient control for DERMS. The proposed BC system enables to securely share DER and grid data among BC clients and acts as a virtual DERMS monitoring and control in the event of a failure of the central DERMS. Compared to [39], this paper provides comprehensive view of the BC governance platform, detailed BC-assisted resilient control algorithms and HLF-based BC system implementation methods. Furthermore, the feasibility of the proposed method is validated by real-time voltage and frequency control recovery case studies in a real-time hardware-in-the-loop (HIL) DER system testbed.

The main contributions of this paper can be summarized as follows:

1) We introduced control schemes for the regulation of voltage and frequency in DERs. These control schemes play a crucial role in maintaining the stability and quality of the electrical grid, particularly in scenarios where DERs are integrated at large scale.
2) We proposed a novel multichannel BC governance platform to establish a cooperative security ecosystem for DERMS. This platform enhances the system's cyber-resilience by integrating BC technology, which ensures secure, decentralized, and tamper-proof data sharing and command distribution, thus protecting against cyber threats.
3) We elaborated on prior work [39] by developing smart contract-based control mechanisms within DERMS. These mechanisms ensure that control commands are reliably sent to each DER when deviations occur due to load changes or voltage/frequency variations, enhancing grid stability and operational efficiency.
4) We implemented a real-time DER co-simulation testbed that integrates a DERMS server, a HLF BC server, IEEE 2030.5 DER network, and gateways, coupled with a real-time grid simulator. This comprehensive testbed allowed us to evaluate the system's performance in a realistic, high-stakes environment, validating the proposed framework's effectiveness.
5) We developed smart contracts for DERMS monitoring and controls, which include frequency and voltage recovery control mechanisms. These smart contracts ensure secure and automated command execution, particularly under conditions of network stress or cyberattack, thereby improving system resilience.

II. RELATED WORKS

A. DERMS AND ATTACK CASES

Figure 1 shows an example of a DERMS interacting with various DERs [40] and an advanced DMS and DERMS cyberattack cases. A DERMS bridges the gap between DER group-level grid service needs from DMS and device level function capabilities from individual DERs. Core capabilities of DERMS include aggregation, translation, simplification, and optimization of the service to the utility, the interest of DER operators, and the lifetime of economics of the DER resources [8]. IEEE 2030.5 network protocol [41] is applied for communications between DERMS and DER systems. The DERMS receives the DER system data such as active power, reactive power, voltage, and frequency measurements and sends the control command such as active power, reactive power and frequency references to DERs for the duration of the service request. The DER aggregator coordinates small DERs as an IEEE 2030.5 server and communicates with the DERMS as a client. DERMS communicate with ADMS using utility network with IEEE 1815 network protocol to provide group-level DER system data to ADMS and receive DER service request such as DER group-level control commands (e.g., power factor setpoints and watt curtailment) and direct commands (e.g., load management and storage dispatch). Detailed DERMS use cases and the roles can be found in [8].

The authors investigated potential attack cases targeting the operational failure of a DERMS in [39], consequently causing the significant loss of visibility and Controllability of the DERs and potentially disrupting the local power grid. A DOS attack is possible if an adversary can keep updating the firewall of a DERMS (i.e., firewall firmware update DOS attack [13]. In addition, discovering the firewall(s) of a DERMS exposed in online via specialized device IP and port search tools (e.g., Shodan) will cause network DOS attacks. Then, the flood of fake requests disables the network devices of the DERMS 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 [13]. The other potential threat is ransomware attacks. For example, a ransomware actor can gain an access to a target DERMS server by purchasing a stolen credential from legitimate insiders, cybercrime partners, or third-party intrusion brokers. Upon obtaining the privileged access, the actor can establish a persistent backdoor in the DERMS server to upload ransomware and export sensitive data [15]. The adversary remotely encrypts the critical files for the DERMS monitoring and control and then starts to demand a significant ransom payment to restore the locked/compromised DERMS. Furthermore, the ex-filtrated data can be exploited to require a more ransom payment, threatening victim employees with an auction or release to the public through an email network. Recovery time from a ransomware attack depends 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.

B. DER CONTROL

In this paper, an IEEE 13 Node Test Feeder circuit with multiple DER sites is considered as a reference DER

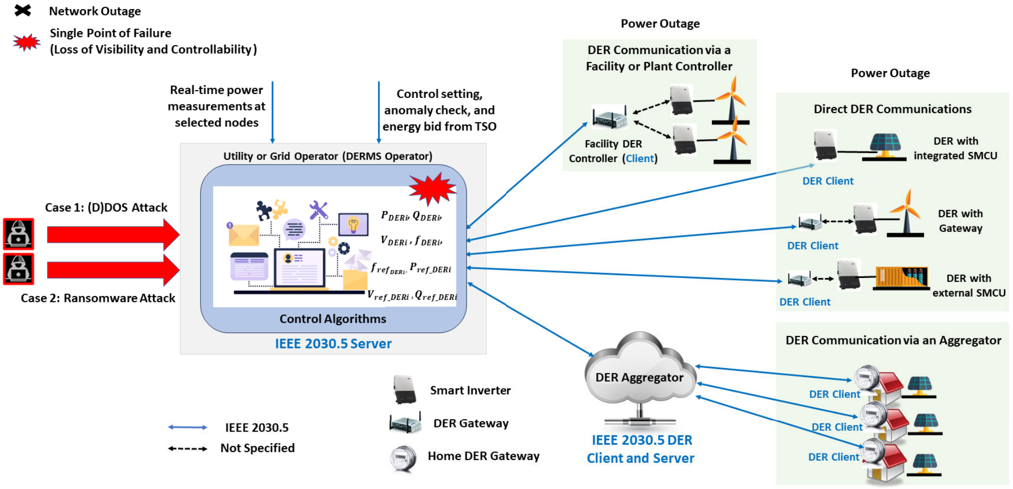

Network Outage
Single Point of Failure
(Loss of Visibility and Controllability)
Real-time power measurements at selected nodes
Control setting, anomaly check, and energy bid from TSO
Utility or Grid Operator (DERMS Operator)
Case 1: (D)DOS Attack
Case 2: Ransomware Attack
P_{DERi}, Q_{DERi},
V_{DERi}, f_{DERi},
$f_{ref_{DERi}}, P_{ref\_DERi}$
$V_{ref\_DERi}, Q_{ref\_DERi}$
Control Algorithms
IEEE 2030.5 Server
Power Outage
DER Communication via a Facility or Plant Controller
Facility DER Controller (Client)
Power Outage
Direct DER Communications
DER with integrated SMCU
DER Client
DER with Gateway
DER Client
DER with external SMCU
DER Client
DER Communication via an Aggregator
DER Aggregator
DER Client
DER Client
DER Client
IEEE 2030.5 DER Client and Server
Smart Inverter
DER Gateway
Home DER Gateway
IEEE 2030.5
Not Specified

FIGURE 1. DERMS integrated at a wide range of DERs and DERMS attack cases.

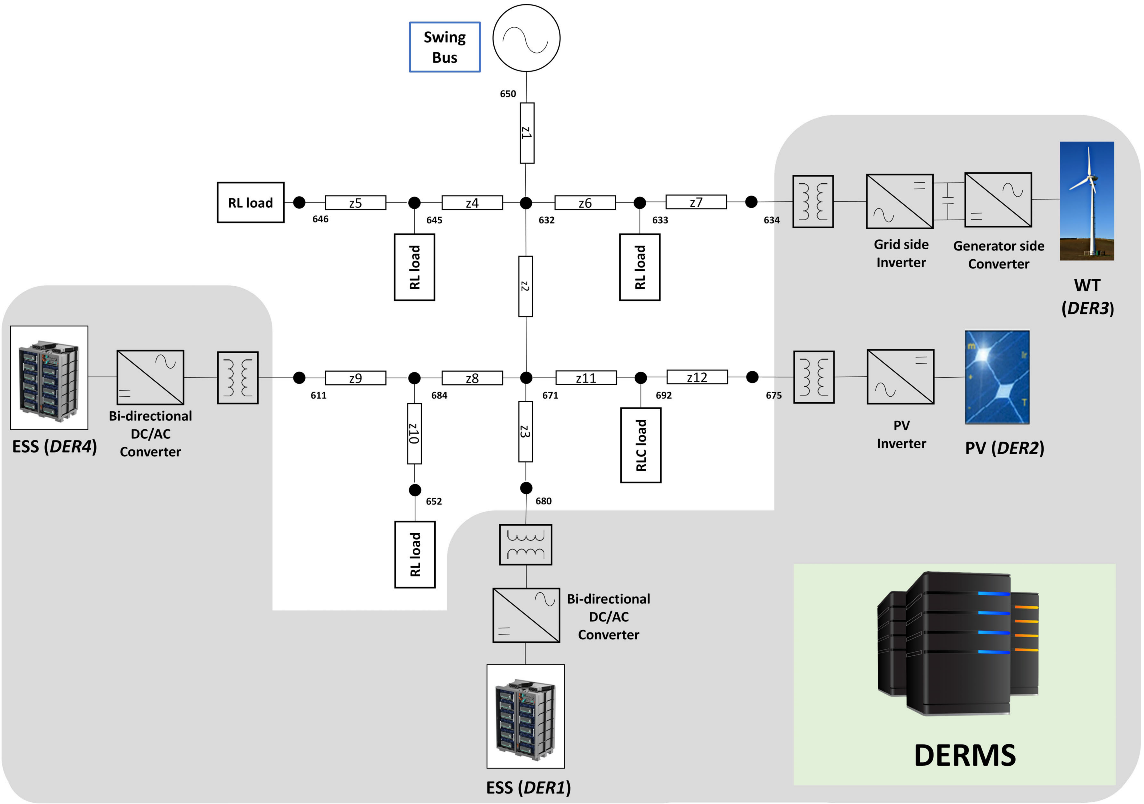


FIGURE 2. A DER System remotely monitored and controlled by a DERMS in an IEEE 13 node test feeder circuit.

system controlled by a DERMS, as shown in Figure 2. The distribution system consists of multiple grid-connected smart inverters for different DERs such as an ESS (DER1), a PV system (DER2), a WT system (DER3), and an ESS (DER4) and several loads. The grid voltage (V_g) at the point of common coupling (PCC) in each DER site can be described as follows:

$$V_g = \frac{di_L}{dt} + V_{\mathrm{inv}} - i_L R \tag{1}$$

where R and L are the series resistance and inductance between the inverter terminal and the PCC; i_L is the inductor current; and V_{inv} is inverter output voltage.

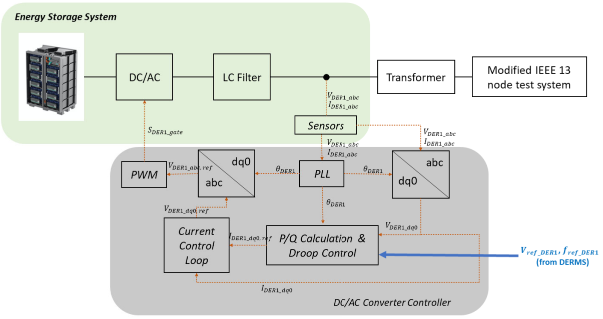


FIGURE 3. ESS control model in IEEE 13 node test feeder circuit.

Figure 3. illustrates the ESS (DER1) control model in IEEE 13 node test feeder circuit where the controller receives the control commands from the DERMS such as frequency reference (f_{ref_DER1}), and voltage reference (V_{ref_DER1}). A droop control is applied for the primary control of the ESS controller, which operates in D-Q (direct and quadrature) frame and the phase of the grid (θ_g) is calculated by a Phase-Locked Loop (PLL). The process by droop control is calculated as follows:

$$P^* = P_{DER1} + K_f(f_{DER1} - f_{\text{DER1}}^{nom}) \tag{2}$$

$$Q^* = Q_{DER1} + K_V(V_{DER1} - V_{\text{DER1}}^{nom}) \tag{3}$$

where P_{DER1} and Q_{DER1} are the measured active power and reactive power at PCC; f_{DER1} is measured frequency at PCC; V_{DER1} is measured voltage at PCC; f_{DER1}^{nom} is nominal frequency of system; V_{DER1}^{nom} is nominal voltage of system; K_f and K_V are the droop coefficients.

The droop control determines D-Q current reference ($i_{\text{dq}}^* = i_{\text{d}}^*$ and i_{q}^*) which can be calculated as follows:

$$i_d^* = \frac{2}{3}\frac{P^*}{V_d} \tag{4}$$

$$i_q^* = -\frac{2}{3}\frac{Q^*}{V_d} \tag{5}$$

where P^* and Q^* are the active and reactive power references and V_d is the measured line voltage.

The current control loop computes D-Q voltage reference ($V_{\text{dq}}^* = V_{\text{d}}^*$ and V_{q}^*) as:

$$V_{\text{d}}^* = (K_P + \frac{K_I}{S})(i_{\text{d}}^* - i_{\text{d}}) - \frac{2\pi f_0 L_f I_{rated}}{V_{rated}} i_{\text{q}} + V_{\text{d}} \tag{6}$$

$$V_{\text{q}}^* = (K_P + \frac{K_I}{S})(i_{\text{q}}^* - i_{\text{q}}) + \frac{2\pi f_0 L_f I_{rated}}{V_{rated}} i_{\text{d}} + V_{\text{q}} \tag{7}$$

where K_P and K_I are parameters of the proportional and integral (PI) control for the internal current loop; i_d and i_q are direct and quadrature axis component of the grid current, respectively; f_0 is nominal frequency and L_f is the inductance of the LC filter; and V_{rated} and I_{rated} are rated voltage and current of *DER1* respectively.

III. BC-ASSISTED DERMS FRAMEWORK

This paper proposes a BC-assisted DERMS framework that enables the DER system to continue to operate during the failure of the DERMS caused by cyberattacks. This section introduces the concept of BC-based cooperative cyber-resilient ecosystem for multiparty-involved DER systems and an overall recovery process.

A. BC-BASED COOPERATIVE CYBER-RESILIENT ECOSYSTEM

Figure 4 shows the concept of BC-based cooperative cyber-resilient ecosystem. For multiparty-involved DER systems environment, establishing a standardized process for mutual agreements using a BC system can facilitate the collaboration of various stakeholders as they advance towards a unified set of robust cyber resilience practices for the DER-rich power grid. The 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 for three types of BC services (i.e., BC channels: Security Channel, Transactive Energy Channel, and Control Channel). For example, 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 and certificates) provided by the vendors using Security Channel, thus providing a viable way to manage the evolving cyber risks on the DER systems. Transactive Energy Channel will be used for record of energy transaction. 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 cyberattacks.

B. BC MODEL FOR A DER SYSTEM

The private BC philosophy primarily includes a distributed ledger platform underpinned by a modular architecture that provides high levels of confidentiality, resilience, flexibility, and scalability between various private business participants. The modular architecture of the BC allows for secure authentication of updates made to the ledger, which can be owned by multiple business partners. In other words, the BC can foster a trustworthy business ecosystem. An illustrative BC business model for DER systems is depicted in Figure 5. Here, a primary host, termed the BC Cluster, encompasses all the comprehensive functionalities of HLF.

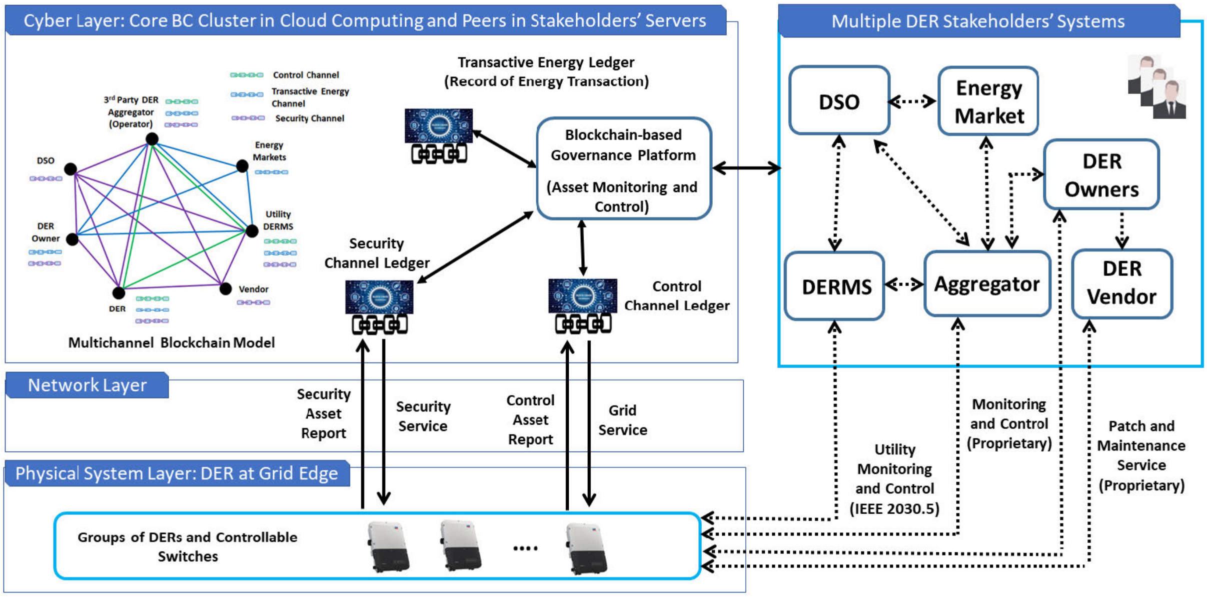

Cyber Layer: Core BC Cluster in Cloud Computing and Peers in Stakeholders' Servers
Control Channel
Transactive Energy Channel
Security Channel
3rd Party DER Aggregator (Operator)
Energy Markets
DSO
Utility DERMS
DER Owner
Vendor
DER
Multichannel Blockchain Model
Transactive Energy Ledger (Record of Energy Transaction)
Blockchain-based Governance Platform
(Asset Monitoring and Control)
Security Channel Ledger
Control Channel Ledger
Network Layer
Security Asset Report
Security Service
Control Asset Report
Grid Service
Physical System Layer: DER at Grid Edge
Groups of DERs and Controllable Switches
Multiple DER Stakeholders' Systems
DSO
Energy Market
DER Owners
DERMS
Aggregator
DER Vendor
Utility Monitoring and Control (IEEE 2030.5)
Monitoring and Control (Proprietary)
Patch and Maintenance Service (Proprietary)

FIGURE 4. Concept of BC-based cooperative cyber-resilient ecosystem for multiparty-involved DER systems.

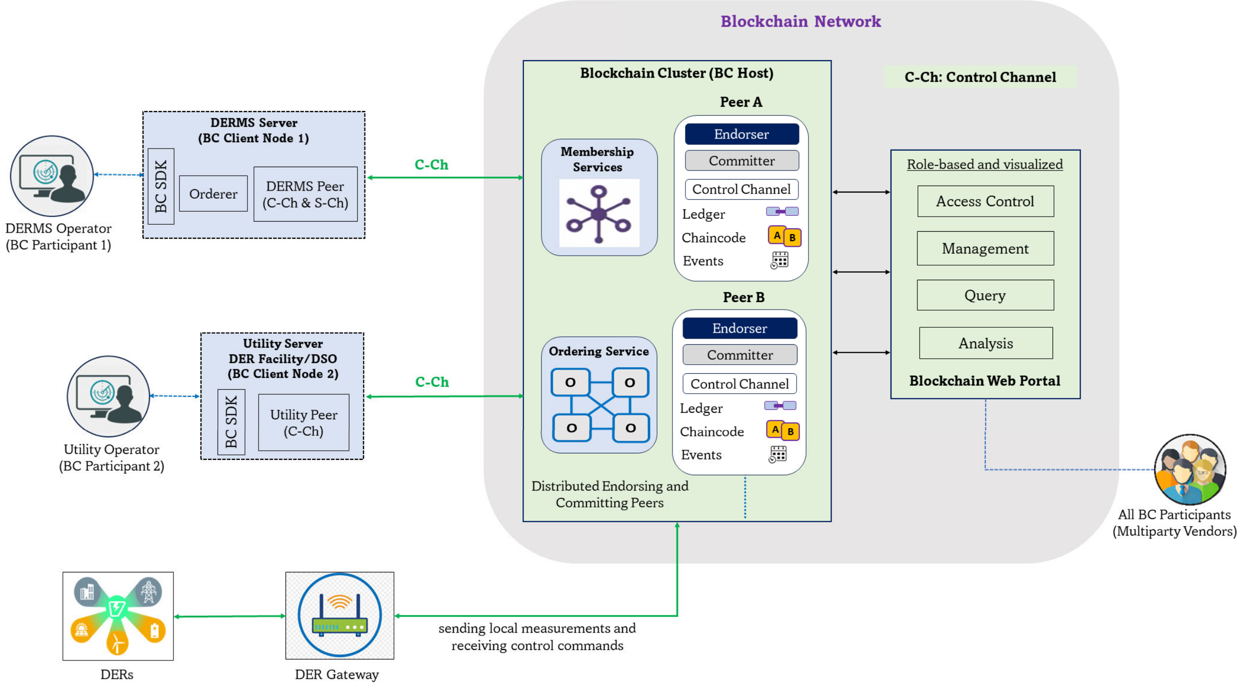


FIGURE 5. BC business model for DER system.

In the BC business network, the DERMS and Utility Operators serve as BC participants using their respective client nodes to interact with the network. The DERMS server includes an orderer and DERMS peer for endorsing and committing transactions, and Utility server includes a utility peer for endorsing transactions related to utility operations. They utilize the HLF Client Software Development Kit (SDK) to create and propose transactions that invoke specific functions on smart contracts, potentially altering the state of the ledger. The transactions are proposed on the Control Channel (C-Ch) for control operations. These proposals are directed to designated endorsing peers, such as Peer A and

Peer B, as determined by a predefined endorsement policy which outlines the necessary endorsements for transaction validity. The endorsing peers simulate the transaction and generate "Read" and "Write" sets (RW sets) that reflect the proposed changes to the ledger, while actual ledger state remains unchanged. This simulation ensures transactions comply with the chaincode's business logic. The endorsers sign the RW sets along with the version numbers of the ledger records involved, verifying the transaction's authenticity. The client application collates these endorsements and forwards the complete transaction package to the ordering service within the network's BC Cluster. The ordering service organizes the transactions into blocks, which are then disseminated across the network to the committing peers for validation. Committing peers verify each transaction against the endorsement policy and the current world state. Valid transactions are then committed to the ledger, updating the world state, while all transactions, regardless of their validity, are recorded on the ledger, ensuring a comprehensive transaction history and maintaining transparency across the network. DER Gateway interfaces with various DERs, sending local measurements and receiving control commands to and from the BC network. Through the BC Web Portal, a role-based and visualized interface, the outcomes of the transactions are conveyed to the client applications. These client applications, associated with the DERMS, and Utility Operators, receive notifications about the transaction results and ledger updates, enabling them to respond accordingly, such as by triggering additional business processes or recording the outcomes for audit purposes, thus maintaining the integrity and transparency of the network's transactional processes.

IV. BC-ASSISTED DERMS FOR CYBER RESILIENCY

Figure 6 illustrates 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 BC peers/nodes are used as a secure medium to deliver critical information in a DER system through the distributed ledgers for secure and resilient control purpose as well as authorized stakeholders for better situational awareness. Connected to the BC 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 DERMS 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 through perturbation and observation (P&O) algorithm-based supervisory control depending on grid conditions. The DERMS smart contract is deactivated once the DERMS recovers. Moreover, an incentive mechanism that provides credits to the peers will be activated, which, however, is not considered in this paper.

V. PROPOSED SMART CONTRACT-DEFINED DERMS CONTROL

Smart contracts are autonomous scripts designed to streamline the execution of written agreements, activating when predetermined conditions are satisfied. BC admins (super users) have a capability of designing and implementing codes in the form of smart contracts for automated DERMS control by providing an interface between the BC network and the physical world (i.e., the DER system). BC participant (clients or nodes) can trigger the smart contract by addressing the transaction. In this paper, a DERMS control is written in smart contract to improve the resiliency of the DER system by the BC network. The proposed smart contract-defined DERMS control consists of two main scripts: 1) *Monitoring script* that describes a rule of data collection and sharing within the BC network including authorized multiparty clients (e.g., DERMS operator and DER owners) and DERs and 2) *Control script* that is a logic statement for DERMS controls. Monitoring script stores DER system data in the control channel ledgers such as $P_{\mathrm{DER}i}, Q_{\mathrm{DER}i}, V_{\mathrm{DER}i}, f_{\mathrm{DER}i}$ $(1 \leq i \leq n)$ as shown in Figure 5. Therefore, the DERMS operators can continuously monitor the status of the DER system by accessing real-time ledger data. Control script generates control commands such as $V_{\mathrm{ref\_DER}i}, f_{\mathrm{ref\_DER}i}, P_{\mathrm{ref\_DER}i}$ and $Q_{\mathrm{ref\_DER}i}$ $(1 \leq i \leq n)$ using the DER system data in the ledgers. Then, each DER can receive/read the updated control commands in the ledger. Therefore, the BC system can work as a virtual DERMS monitoring and control on behalf of the DERMS.

Algorithm 1 governs the control procedures for frequency and voltage recovery at the PCC in the DER system. The algorithm initiates by collecting voltage and current data from each DER and monitoring the system for power outages and supervisory control signals. It calculates the frequency error from the current DER frequency to the nominal value. If the error deviation exceeds a threshold ($\Delta\varepsilon_f$), the system applies corrective actions, adjusting the frequency within the defined "min" and "max" limits (e.g., ±1.5 pu). This ensures that frequency adjustments remain within safe operational bounds. Similarly, the algorithm calculates voltage error from the current voltage to the desired voltage. If the voltage error deviation exceeds threshold ($\Delta\varepsilon_v$), the voltage reference is adjusted incrementally, again within the same ±1.5 pu limits. Once the adjustments are made, the control instructions are sent to each DER, ensuring that both frequency and voltage corrections are applied to maintain stability during disturbances.

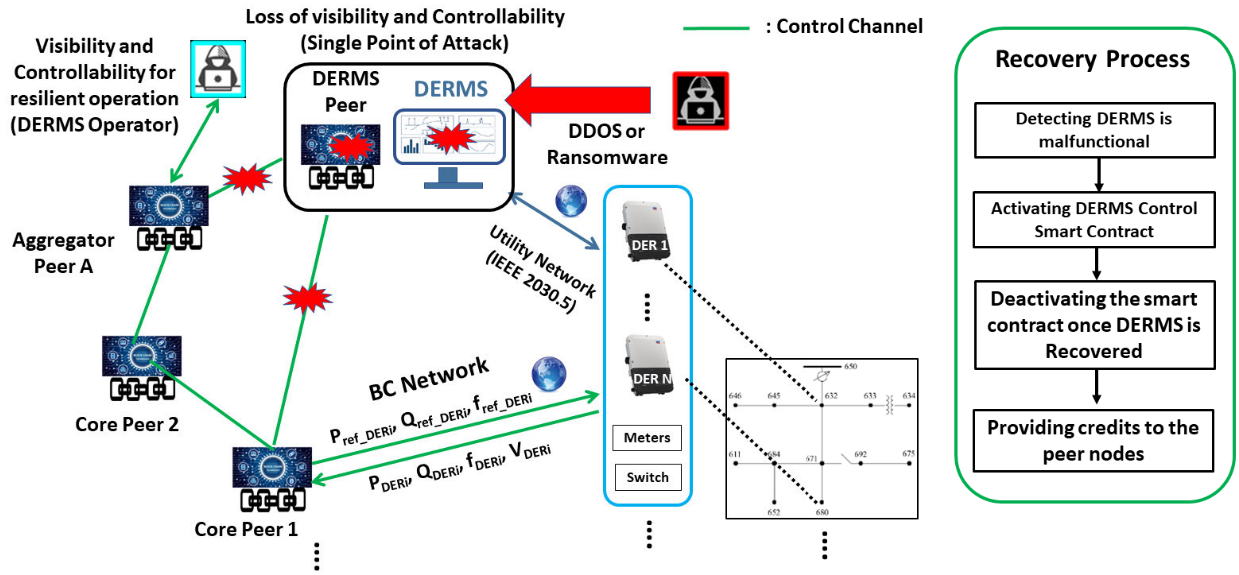

Visibility and Controllability for resilient operation (DERMS Operator)
Loss of visibility and Controllability (Single Point of Attack)
DERMS Peer
DERMS
: Control Channel
DDOS or Ransomware
Aggregator Peer A
Utility Network (IEEE 2030.5)
DER 1
DER N
Meters
Switch
BC Network
Core Peer 2
Core Peer 1
P_ref_DERi, Q_ref_DERi, f_ref_DERi
P_DERi, Q_DERi, f_DERi, V_DERi
Recovery Process
Detecting DERMS is malfunctional
Activating DERMS Control Smart Contract
Deactivating the smart contract once DERMS is Recovered
Providing credits to the peer nodes

FIGURE 6. Proposed BC-assisted resilient DERMS controlled by DERMS control smart contract and an overall recovery process of the malfunctional DERMS.

A. SMART CONTRACT-DEFINED FREQUENCY CONTROL

The frequency control mechanism for DERs involves measuring the frequency at the PCC and comparing it with the nominal frequency to form a reference for error adjustments. This reference is used to adjust the frequency error, ensuring that the system operates within the desired stability range. Additional step adjustments are made using the P&O algorithm to ensure convergence within the stability range. Instead of using the nominal frequency as the operating point, the DER performs droop control by setting the provided reference as the new operating point. The frequency control equation in (2) is reformulated to incorporate these adjustments, ensuring that the DERs can effectively respond to frequency deviations and maintain grid stability.

$$P^* = P_{\mathrm{DER}i} + K_f(f_{\mathrm{DER}i} - f_{\mathrm{ref\_DER}i}) \tag{8}$$

where $f_{\mathrm{ref\_}DERi}$ is the updated frequency reference from the DERMS; and P^* and Q^* are the active power reference and reactive power reference, respectively. However, when applying the P&O algorithm, step-induced ripples occur. To mitigate the ripples, control is only executed when a certain threshold $\Delta\varepsilon_f$ is violated.

B. SMART CONTRACT-DEFINED VOLTAGE CONTROL

The voltage control follows the same structure as the previous frequency control. Generally, voltage stability is more influenced by the adjustment of reactive power than active power. As a result, the voltage regulation using the P&O algorithm causes the DER to adjust its reactive power output. Therefore, Eq. (3) is defined as follows:

$$Q^* = Q_{\mathrm{DER}i} + K_v(V_{\mathrm{DER}i} - V_{\mathrm{ref\_DERi}}) \tag{9}$$

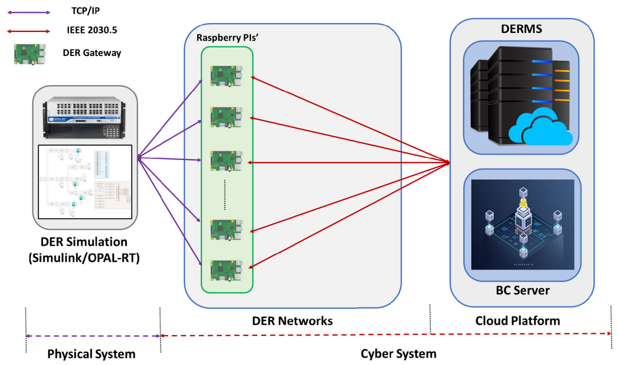


FIGURE 7. A diagram of the real-time HIL DER system and BC system co-simulation testbed.

where $V_{\mathrm{ref\_}DERi}$ is the updated frequency reference from the DERMS; and P^* and Q^* represent the active power and reactive power references, respectively. Additionally, voltage regulation is performed only when the error exceeds the threshold $\Delta\varepsilon_v$ to adjust the ripple.

VI. REAL-TIME HIL DER AND BC CO-SIMULATION TESTBED

This section provides details about the proposed real-time HIL DER system and BC system co-simulation testbed, as shown in Figure 7. This testbed mainly includes: 1) a real-time DER physical system simulator, 2) a real DER cyber system consisting of network devices, DER gateways, a DERMS server, and 3) a BC system. The DERMS Server and DER gateways are implemented in Raspberry Pi 4Bs while the BC system is implemented in a Linux-based PC.

Algorithm 1 DERMS Control Procedure

```
Initialize model parameter
Monitor and collect $V_{DER_i}^{means}$ and $f_{DER_i}^{means}$ for each DER
if Power Outage is ON then
    if Supervisory Control Signal is ON then
        if $\Delta t_{step} = 10$ msec then
            Frequency Error $\Delta f = f_{DER}^{means} - f_{DER}^{nom}$
            Error Deviation $\Delta\theta_f = \Delta f - \Delta f^{t-1}$
            if $\| \Delta\theta_f \| > \Delta\varepsilon_f$ then
                if $(f_{DER}^{means} < f_{min}$ and $\Delta f > 0)$ or $(f_{DER}^{means} < f_{max}$ and $\Delta f < 0)$ then
                    $f_{DER}^{*,t} = f_{DER}^{*,t-1} + f_{step}$
                end if
                if $(f_{DER}^{means} < f_{min}$ and $\Delta f < 0)$ or $(f_{DER}^{means} > f_{max}$ and $\Delta f < 0)$ then
                    $f_{DER}^{*,t} = f_{DER}^{*,t-1} - f_{step}$
                end if
                Update Frequency Reference $f_{DER}^{*,t}$
            end if
        end if
        if $\Delta t_{step}$ = 100 msec then
            Voltage Error $\Delta V = V_{DER}^{means} - V_{DER}^{nom}$
            Error Deviation $\Delta\theta_V = \Delta V - \Delta V^{t-1}$
            if $\| \Delta\theta_V \| > \Delta\varepsilon_V$ then
                if $(V_{DER}^{means} < V_{min}$ and $\Delta V > 0)$ or $(V_{DER}^{means} < V_{max}$ and $\Delta V < 0)$ then
                    $V_{DER}^{*,t} = V_{DER}^{*,t-1} + V_{step}$
                end if
                if $(V_{DER}^{means} < V_{min}$ and $\Delta V < 0)$ or $(V_{DER}^{means} > V_{max}$ and $\Delta V < 0)$ then
                    $V_{DER}^{*,t} = V_{DER}^{*,t-1} - V_{step}$
                end if
                Update Voltage Reference $V_{DER}^{*,t}$
            end if
        end if
        Each DER ← Frequency and Voltage Reference
    end if
end if
```

A. DER SYSTEM MODELING AND GRID SIMULATION

The real-time DER physical system simulator operates the DER system in the IEEE 13 Node Test Feeder circuit in Figure 2. The bus frequency is 60Hz and the nominal voltage is 4.16 kV. Inverters of WT and PV systems perform maximum power point tracking (MPPT) controls. The WT of the 634 bus is applied with the permanent magnet synchronous generator (PMSG) model and the rated power is 2.2 MVA. The PV is located on bus 675 and the rated output is 1MW. The ESS capacity of bus 680 and 646 is 1 MWh and a lithium-ion battery model is used. Except for the bus where the generators are connected, the resistive, inductive, and capacitive loads are evenly connected to other buses, where the real power demand of the distribution system is 3.5 MW. The reactive power demand of inductive and capacitive loads are 2.102 and 0.7 MVAR, respectively. The impedance values between the buses are chosen based on the IEEE 13 bus system. The DER system model is implemented in MATLAB/Simulink where each DER is connected to its subsequent gateway through TCP/IP.

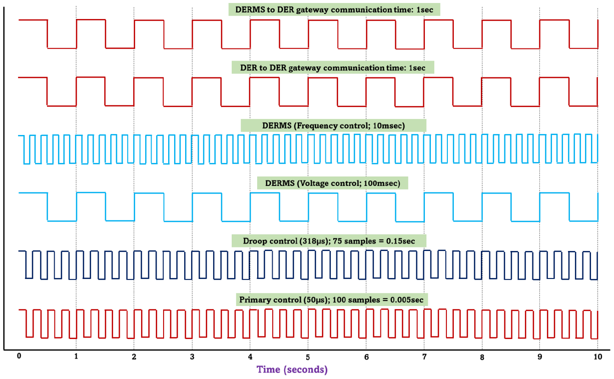


FIGURE 8. Communication and control time frame.

The communication and control signals used in the system is shown in Figure 8. The top waveform (in red) represents the communication from the DERMS to the DER Gateway, occurring every 1 second. This indicates a regular interval at which the DERMS sends updates or commands to the DER Gateway. The second waveform (also in red) likely represents the communication from the DERs to the DER Gateway, also occurring every second. This suggests that the DERs are sending status updates such as voltage, current, and power measurements to the gateway. The third waveform (in blue) shows the DERMS frequency control actions, occurring every 10 milliseconds, which is typical for maintaining grid stability. Voltage control is essential for maintaining voltage levels within the desired range. The fifth waveform (in light blue) represents droop control with a sampling time of 320 microseconds. The diagram shows 75 samples over 0.15 seconds for better visualization. PLL control measurements are passed through a 500 Hz low pass filter, allowing broader control than the inverter's internal control, indicating refined system adjustments. The bottom waveform (in red) displays the inverter's control actions in 50 microsecond increments. The diagram shows 100 samples over 0.005 seconds for visualization. This control generates a voltage waveform for PWM control of the inverter, with references from droop control.

B. REAL-TIME DER CYBER SYSTEM

The real-time cyber system of our HIL co-simulation testbed consists of DER gateways (one for each DER in the system model), a DERMS server and a BC server. A custom-made IEEE 2030.5-2018 network with TLS 1.3 was implemented between the DERMS server and DER gateways. Thus, we generated a custom-made certificate authority (CA) for providing Root-CA public key to sign and generate certificates for both DERMS and DER gateways. Also, we leveraged docker platform for deploying and running the applications involved in DERMS and BC servers, such that lightweight runtime is achieved for these servers. Each of these elements of the proposed cyber system are detailed as follows:

1) DER GATEWAYS

DER gateway is connected to DER system model through TCP/IP-based local network. The DER gateway is a simple Python-3 based TCP/IP application that acts as an exchange medium between DER system model and both DERMS and BC servers. From a client-server perspective, it is a common client for both DERMS and BC servers which relays the real-time DER data from DER system model. The other functionality of this DER gateway is that it also relays the control commands from both DERMS and BC servers to DER system model.

2) DERMS SERVER

The DERMS server receives the DER data from the corresponding DER gateway and sends control commands to subsequent DER gateway using the IEEE 2030.5-2018 network. The DERMS server comprises two interdependent Docker containers: TLS 1.3-based Nginx container and a DERMS web-application container. To comply with the technical requirements of IEEE 2030.5-2018 standard, we utilized Python-3 and Flask REST framework for developing the DERMS web-application, whereas the Nginx is programmed to use TLS 1.3 and previously generated DERMS server certificates for communication. The Nginx container is the entry-point for all the incoming client connections/requests ensuring the HTTPS (TLS) communication, where the incoming request is decrypted and data is sent to the DERMS web-application container. The DERMS web-application container processes the incoming real-time DER data and saves it in a local SQLite3 database, that is not accessible to any other docker container or application running on that machine. DER data saved in the database is mapped to each DER using Short Form Device Identifier (SFDI) and real-time plots for monitoring each DER is generated using the Python module pyplot from matplotlib.

C. BC SYSTEM

As discussed in the functionality of DER gateway, similar to the DERMS server, the BC server also receives the DER data from the corresponding DER gateway and responds back with control commands to the subsequent DER gateway. The BC server comprises of a REST API (docker container) and a BC network (docker network) that consists of docker containers for CAs, Orderers, and Peers. We developed the REST API using Go programming language and REST framework and used the previously generated BC server certificates for communication, whereas the BC network is established using HLF. We defined the HLF topology as one organization that comprises of one Orderer node, one Peer node and one channel for internal HLF communications. We used the HLF service called Fabric CA, to create separate CAs for the Orderer and the organization and this service by default uses elliptic curve cryptography (ECC) algorithm (with SECP256R1 curve) for generating certificates. Using the organization CA, we generated the Membership Service Provider (MSP) for Peers, Users and organization administrator, and certificates for Peers, whereas using the Orderer CA, we generated the MSP for Orderer and administrator, and certificates for Orderer. After generating these MSPs and certificates, we created the channel and registered the Peers to the channel, and configured an Anchor Peer for the organization using the organization administrator MSP. Once, all these configurations are finalized, we deployed the chaincode on to the Peers, so that clients can connect to BC network and submit BC transactions for processing.

The REST API of BC server is actually a client for the HLF-based BC network and uses the organization administrator MSP for connecting to the peer in order to submit the BC transactions. Similar to Nginx container of DERMS server, the REST API of the BC server is the entry-point for all the incoming connections/requests which decrypts the DER data from DER gateway and sends to the BC network for processing. The BC network processes the DER data based on the BC transaction (of the chaincode) invoked and sends the control response back to the REST API, which is relayed to DER gateway. Thus, enabling BC network accessible to external entities for submitting BC transactions.

VII. VALIDATION

In this section, we validated the effectiveness of the proposed BC-assisted resilient DERMS control framework using the proposed testbed described in Section VI. Figure 9 illustrates the experimental testbed. The grid simulation model described in Section VI-A, includes a diverse load change profile across multiple buses. After 6 seconds, loads connected to buses 633 and 634 were reduced from 900 kW/640 kVAr to 680 kW/520 kVAr; buses 652 and 611 were configured with increased load demands rising from 90 kW/40 kVAr to 10 kW/10 kVAr and from 250 kW/160 kVAr to 550 kW/320 kVAr, respectively; and buses 645 and 646 adjusted connected loads from 250 kW/130 kVAr to 600 kW/340 kVAr. This variation in load levels creates a realistic testing environment that reflects potential challenges in maintaining grid stability under operational disruptions and dynamically changing load profiles.

Various operating conditions were tested to evaluate the performance of the proposed system in different scenarios. The validation includes: 1) real-time monitoring and controlling capability of the DERMS platform, 2) grid impact simulation using the testbed during the DERMS outages, 3) assessing the resiliency of the proposed BC-assisted resilient DERMS control method; and 4) comparison of the proposed method with other recent BC approaches for DERs.

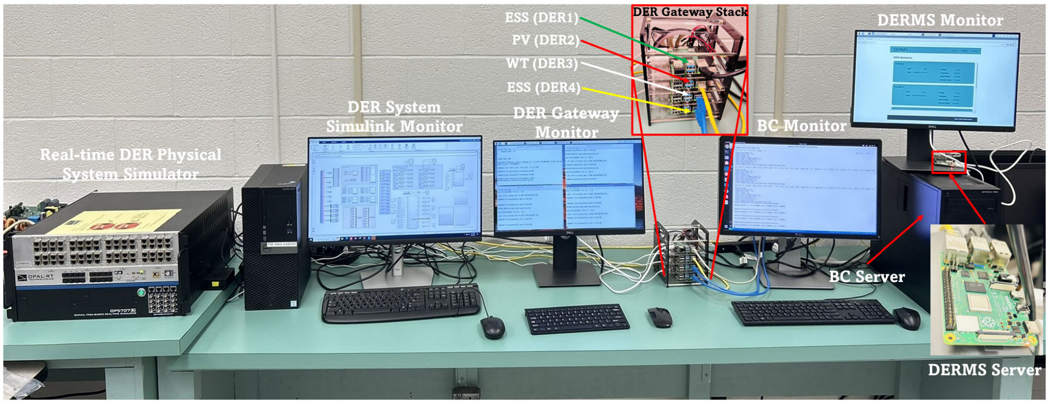


FIGURE 9. Experimental testbed.

A. REAL-TIME MONITORING AND CONTROL OF DERMS SERVER

A real-time monitoring and control of the centralized DERMS server was validated first. Figure 10 illustrates the visualized real-time data from PV, WT and ESS in the DERMS platform sent by the DER Gateways. The monitoring DER data includes $V_{\mathrm{DER}i}, f_{\mathrm{DER}i}, P_{\mathrm{DER}i}, Q_{\mathrm{DER}i}$ where i represents the number of DERs ($1 \leq i \leq 4$). It is observed that the DERMS server can continuously collect data from the connected DERs and it executes the DERMS control algorithms to ensure grid stability by sending timely control commands to the DERs.

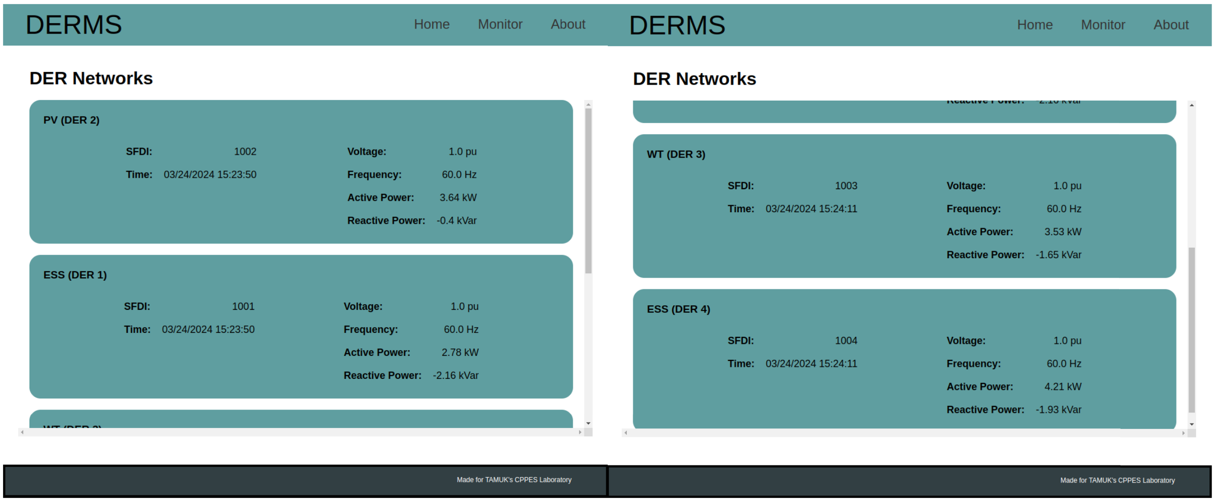
B. GRID IMPACT OF DERMS OUTAGE AND RECOVERY USING BC-ASSISTED RESILIENT DERMS

To assess the consequences of a centralized DERMS outage in the distribution grid, we conducted experiments with the scenarios where the DERMS experienced disruptions due to cyberattacks. After a network reconfiguration is performed (0-1 second), an immediate DERMS is performed to take control at 1 second, but the DERMS maintains the old references from the cyberattack and is unable to configure the correct references to respond to load variations. The impact on the distribution grid includes both frequency and voltage instability as shown in Figure 11 and Figure 12, respectively. These disruptions highlighted the critical role of the DERMS in maintaining grid stability and the potential risks associated with centralized control systems being compromised.

Figure 11 illustrates the impact of a cyberattack on a DERMS and its subsequent effects on grid stability. It shows frequency variations over time under different operational conditions. During normal operation (0-4 seconds time period), the frequency remained relatively stable around 60 Hz, with minor fluctuations. The sudden frequency drop at the 4-second mark demonstrates the immediate and severe impact of the cyberattack on grid stability. This aligns with the scenario description where the DERMS maintains incorrect references after the attack, unable to respond properly to load variations. When the cyberattack occurred (4-10 seconds time period), a significant drop in frequency across all four DER units was observed, indicating grid instability. At the 10-second mark, the activation of BC-assisted DERMS control restored the frequency stability, with all DERs returning to near-nominal frequencies. The result demonstrates that the effectiveness of the proposed BC-assisted DERMS frequency control in managing and mitigating the impacts of frequency oscillations caused by the central DERMS outage.

Figure 12 illustrates the voltage response of four DERs under various conditions: normal operation, outage due to cyberattack, and the activation of a BC-assisted DERMS control. For the initial 4 seconds, the DERs were in a operation under normal DERMS control with minor fluctuations around their nominal values. However, starting at 4 seconds, a cyberattack disrupted the DERMS, causing significant voltage instability across all DERs, particularly noticeable in DER1 and DER2, with DER3 and DER4 also exhibiting considerable changes. This period highlights the grid's vulnerability to cyber threats and the critical role of DERMS in maintaining voltage stability. After 10 seconds, the activation of BC-assisted DERMS control restored voltage stability, with all DERs returning to near-nominal values. This result clearly demonstrates the efficacy of the proposed BC-assisted resilient voltage control mechanism in managing and mitigating the impacts of cyberattacks and other disturbances.

Figure 13 displays the voltage response at 12 different buses in a power distribution network during three operational phases: normal DERMS operation, a DERMS outage due to cyberattack, and the execution of a BC-assisted DERMS control. From 0 to 4 seconds, the DERMS operates normally, maintaining stable voltage levels around 1 p.u. across all buses. This phase shows minor fluctuations, indicating the typical operational variances within acceptable limits. At the 4-second mark, a cyberattack disrupts the DERMS, leading to significant voltage instability. The voltages at various buses deviate from their nominal values, with some dropping below 0.8 p.u. and others rising above 1.2 p.u. This period, lasting



DER Networks

PV (DER 2)

SFDI:	1002	Voltage:	1.0 pu
Time:	03/24/2024 15:23:50	Frequency:	60.0 Hz
		Active Power:	3.64 kW
		Reactive Power:	-0.4 kVar

ESS (DER 1)

SFDI:	1001	Voltage:	1.0 pu
Time:	03/24/2024 15:23:50	Frequency:	60.0 Hz
		Active Power:	2.78 kW
		Reactive Power:	-2.16 kVar

Made for TAMUK's CPPES Laboratory

DER Networks

WT (DER 3)

SFDI:	1003	Voltage:	1.0 pu
Time:	03/24/2024 15:24:11	Frequency:	60.0 Hz
		Active Power:	3.53 kW
		Reactive Power:	-1.65 kVar

ESS (DER 4)

SFDI:	1004	Voltage:	1.0 pu
Time:	03/24/2024 15:24:11	Frequency:	60.0 Hz
		Active Power:	4.21 kW
		Reactive Power:	-1.93 kVar

Made for TAMUK's CPPES Laboratory

FIGURE 10. Real-time DER monitoring in the DERMS platform.

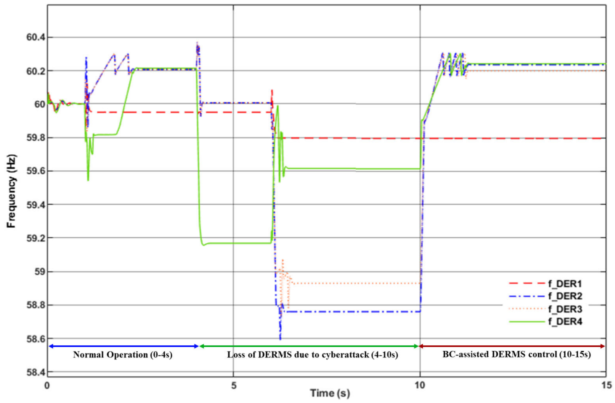


FIGURE 11. Frequency stability response of DERs.

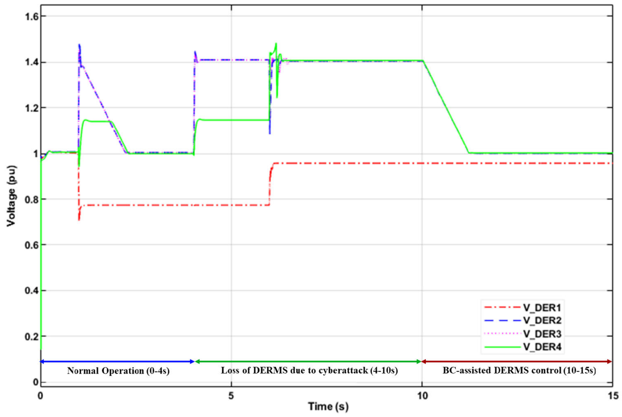


FIGURE 12. Voltage stability response of DERs.

until 10 seconds, highlights the system's vulnerability to cyber threats, causing considerable voltage instability and variation across the network. At 10 seconds, the BC-assisted DERMS control is activated, successfully restoring voltage stability across all buses. The voltages return to near-nominal values, demonstrating the effectiveness of the BC-assisted DERMS in mitigating the impacts of the cyberattack and re-establishing stable operation.

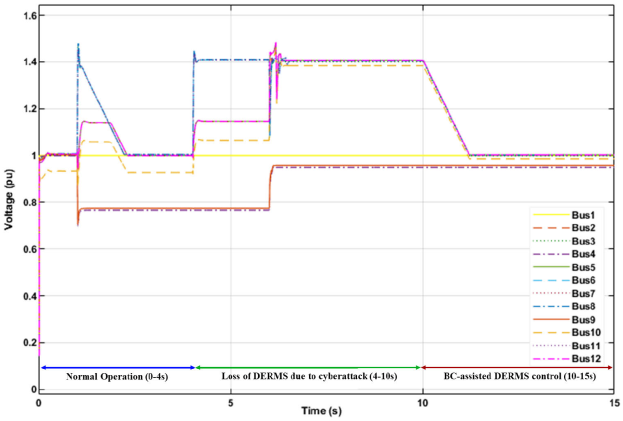


FIGURE 13. Voltage stability at buses 1-12 within an electrical distribution network.

Overall, these results underscore the importance of resilient and advanced control systems in maintaining both voltage and frequency stability in power distribution networks, particularly in the face of cyber threats. The use of BC technology in the DERMS control shows its potential to enhance grid resilience and security, ensuring stable voltage and frequency levels across DERs and buses even during cyberattacks. This highlights the critical role of BC-assisted DERMS control in mitigating the adverse effects of cyberattacks, thereby enhancing the overall reliability and security of the power distribution network.

C. COMPARISON

Table 1 shows the comparison of the proposed method with other recent BC approaches for DERs [42], [43], [44], [45] for DERs in terms of application, usage of smart contract,

TABLE 1. Comparison of the proposed method with other recent BC approaches for DERs.

Aspect	This Paper	[42]	[43]	[44]	[45]
Application	Secure virtual DERMS	Wireless sensor network for secure DER monitoring and control	Secure transactive control in load frequency control (LFC) markets in a renewable-based hybrid power system	Secure Vehicle-to-vehicle (V2V) energy trading in renewable energy integration	Peer-to-peer (P2P)trading in microgrids
Smart Contracts	DER monitoring and control (frequency and voltage control)	BC node access control	Transactive control in LFC markets	Energy trade	Double auction mechanism
BC Platform	HLF	Custom-made BC program	Custom-made BC program	HLF	Ethereum
Validation	Real-time HIL (grid impact and real DERMS and BC servers)	Simulation (BC performance)	Simulation (grid impact)	Simulation (BC performance, real BC server)	Real-time HIL (grid impact and real BC server)

type of BC platform, and validation method. Most of articles utilized BC technology for general BC applications such as secure communication [42] and energy transactions [43], [44], [45]. However, this paper focuses on developing a secure virtual DERMS acting as a real DERMS and enhancing DER system resilience, specifically when a central DERMS is in DOS status in addition to secure BC communication and transactions. Moreover, the proposed virtual DERMS has been developed in a real HLF platform and tested in a real-time HIL DER testbed with a real DERMS server, providing more realistic grid environment and impact. However, most of articles only demonstrated their proposed method in a simulation environment [42], [43], [44]. This comparison clearly highlights that the proposed BC-assisted DERMS framework and its testbed are uniquely positioned compared to peers.

VIII. CONCLUSION

This paper explored an overview of BC-based governance model for future cyber-secure and resilient DER systems in a multiparty involved environment. Furthermore, this paper introduced a single point of failure vulnerability in the current centralized DERMS caused by cyberattacks. To address the threat of cyberattacks targeting the DERMS, this paper has proposed a BC-assisted resilient control for DERs. Therefore, distributed DERs can be continuously monitored and controlled by the proposed BC-assisted control as a vitual DERMS during the central DERMS outage or under attacks. The proposed BC-assisted resilient control method is validated in a real-time HIL and validate the grid resiliency through frequency and voltage recovery controls. Future works include: 1) investigation of next-generation BC framework for secure and sustainable energy trading in the metaverse; 2) ensemble learning for intrusion detection in SDN-based zero-touch smart grid systems; and 3) BC-based reverse auction for V2V charging in smart grid environments.

REFERENCES

[1] B. Kroposki, B. Johnson, Y. Zhang, V. Gevorgian, P. Denholm, B.-M. Hodge, and B. Hannegan, "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," *IEEE Power Energy Mag.*, vol. 15, no. 2, pp. 61–73, Mar. 2017.

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

[3] M. Obi, T. Slay, and R. Bass, "Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards," *Energy Rep.*, vol. 6, pp. 2358–2369, Nov. 2020, doi: 10.1016/j.egyr.2020.08.035.

[4] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547-2018, (Revision IEEE Standard 1547-2003), 2018, pp. 1–138, doi: 10.1109/IEEESTD.2018.8332112.

[5] J. Wang, J. Simpson, R. Yang, B. Palmintier, S. Tiwari, and Y. Zhang, "Hardware-in-the-loop evaluation of an advanced distributed energy resource management algorithm," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, 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. 18th Int. Conf. Smart Technol. (IEEE EUROCON)*, Jul. 2019, pp. 1–5.

[7] *IEEE Guide for Distributed Energy Resources Management Systems (DERMS) Functional Specification*, IEEE Standard 2030.11-2021, 2021, pp. 1–61.

[8] B. Seal, A. Renjit, and B. Deaver, "Understanding DERMS," Electr. Power Res. Inst., Palo Alto, CA, USA, Tech. Rep. 3002013049, Jul. 2018.

[9] A. Energy, "Distributed energy resource (DER) strategy, next steps, and preliminary findings from Austin SHINES DER integration project," Tech. Rep., 2021.

[10] (Aug. 2018). *AutoGrid—DERMS Software. Flexibility Delivered. Proven Results*. Accessed: Nov. 23, 2023. [Online]. Available: https://www.auto-grid.com/

[11] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, and J. T. Johnson, "Cyber security primer for der vendors aggregators and grid operators," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND-2017-13113; 674083, Nov. 2017. [Online]. Available: https://www.osti.gov/biblio/1761987, doi: 10.2172/1761987.

[12] B. Ahn, T. Kim, J. Choi, S.-w. Park, K. Park, and D. Won, "A cyber kill chain model for distributed energy resources (DER) aggregation systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.

[13] *Denial of Service Condition' Disrupted U.S. Energy Company Operations*. Accessed: Dec. 16, 2024. [Online]. Available: https://techcrunch.com/2019/05/02/ddos-attack-california-energy/

[14] S. Larson and C. Singleton, "Singleton, ransomware in ICS environments," Dragos, Hanover, MD, USA, White Paper, 2020.

[15] Y. Su, B. Ahn, S. R. B. Alvee, T. Kim, J. Choi, and S. C. Smith, "Ransomware security threat modeling for photovoltaic systems," in *Proc. 6th IEEE Workshop Electron. Grid (eGRID)*, Nov. 2021, pp. 1–5.

[16] J. Henry, "Cyber security requirements and recommendations for CSIRD& D solicitation #4 distributed energy resource communications," Electr. Power Res. Inst., Los Angeles, CA, USA, Tech. Rep. CPU0267.01, 2015.

[17] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Nat. Lab, Albuquerque, NM, USA, Sandia Tech. Rep. SAND2017-13262, 2017.

[18] D. Saleem and C. Carter, ''Certification procedures for data and communications security of distributed energy resources,'' Nat. Renew. Energy Lab., Golden, CO, USA, Tech. Rep. NREL/TP-5R00-73628, Jul. 2019. [Online]. Available: https://www.osti.gov/biblio/1545269

[19] 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-Phys. Syst., Theory Appl.*, vol. 5, no. 3, pp. 274–282, Sep. 2020.

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

[21] 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.

[22] 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, pp. 1322–1334, Mar. 2022.

[23] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, ''Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[24] A. Chavez, C. Lai, N. Jacobs, S. Hossain-McKenzie, C. B. Jones, J. Johnson, and A. Summers, ''Hybrid intrusion detection system design for distributed energy resource systems,'' in *Proc. IEEE CyberPELS (CyberPELS)*, Apr. 2019, pp. 1–6.

[25] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, ''Cybersecurity for distributed energy resources and smart inverters,'' *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, Dec. 2016. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-cps.2016.0018, doi: 10.1049/iet-cps.2016.0018.

[26] N. Prusty, ''`it's like the early days of the internet,' Blockchain-based Brooklyn microgrid tests P2P energy trading,'' Microgrid Media, Irvine, CA, USA, Mar. 2016.

[27] American Public Power Association. *Blockchain REC Trading Platform Set to Launch in the U.S.* Accessed: Dec. 16, 2024. [Online]. Available: https://www.publicpower.org/periodical/article/blockchain-rec-trading-platform-set-launch-us

[28] 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, p. 2024, Mar. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/6/2024

[29] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, ''Centralized and decentralized distributed energy resource access control implementation considerations,'' *Energies*, vol. 15, no. 17, p. 6375, Sep. 2022.

[30] M. E. Mylrea and S. N. G. Gourisetti, ''Blockchain: Next generation supply chain security for energy infrastructure and nerc critical infrastructure protection (cip) compliance,'' *J. Systemics, Cybern. Inform.*, vol. 16, no. 6, pp. 1–9, Jun. 2018. [Online]. Available: https://www.osti.gov/biblio/1508134

[31] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim, ''Blockchain-based man-in-the-middle (MITM) attack detection for photovoltaic systems,'' in *Proc. IEEE Design Methodol. Conf. (DMC)*, Jul. 2021, pp. 1–6.

[32] J. Choi, B. Ahn, S. Pedavalli, S. Ahmad, A. Villasenor, and T. Kim, ''Secure firmware update and device authentication for smart inverters using blockchain and phyiscally uncloable function (PUF)-embedded security module,'' in *Proc. 6th IEEE Workshop Electron. Grid (eGRID)*, Nov. 2021, pp. 1–4.

[33] A. A. Hadi, G. Bere, B. Ahn, and T. Kim, ''Smart contract-defined secondary control and co-simulation for smart solar inverters using blockchain technology,'' in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–6.

[34] S. Alliance. *Blockchain to Record Private Key Properties in DER Equipment*. Accessed: Dec. 16, 2024. [Online]. Available: https://sunspec.org/wp-content/uploads/2021/03/SunSpecAlliance

[35] F. Rahimi, ''Blockchain transactive energy (BCTE) position paper,'' IEEE Position Vis. Statement Paper, Tech. Rep., 2021.

[36] J. Wang, J. Simpson, R. Yang, B. Palmintier, S. Tiwari, and Y. Zhang, ''Performance evaluation of an advanced distributed energy resource management algorithm,'' in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 378–384, doi: 10.1109/SmartGridComm51999.2021.9632298.

[37] J. Wang, J. Huang, and X. Zhou, ''Performance evaluation of distributed energy resource management algorithm in large distribution networks,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2021, pp. 1–5.

[38] J. Wang, M. Blonsky, F. Ding, S. C. Drew, H. Padullaparti, S. Ghosh, I. Mendoza, S. Tiwari, J. E. Martinez, J. J. D. Dahdah, F. A. M. Bazzani, M. Baggu, M. Symko-Davies, C. Bilby, and B. Hannegan, ''Performance evaluation of distributed energy resource management via advanced hardware-in-the-loop simulation,'' in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[39] S. Ahmad, B. Ahn, T. Kim, J. Choi, M. Chae, D. Han, and D. Won, ''Blockchain-integrated resilient distributed energy resources management system,'' in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2022, pp. 59–64.

[40] J. Kim, K. Park, B. Ahn, J. Chor, 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. IEEE PES Innov. Smart Grid Technol.-Asia (ISGT Asia)*, Dec. 2021, pp. 1–5.

[41] IEEE Standards Association. (2018). *IEEE Standard for Smart Energy Profile Application Protocol*. Accessed: Nov. 20, 2023. [Online]. Available: https://standards.ieee.org/standard/20305-2018.html

[42] M. Faheem, B. Raza, M. S. Bhutta, and S. H. H. Madni, ''A blockchain-based resilient and secure framework for events monitoring and control in distributed renewable energy systems,'' *IET Blockchain*, Jun. 2024.

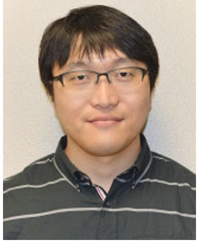
[43] R. Loka, A. M. Parimi, S. T. P. Srinivas, and N. M. Kumar, ''Leveraging blockchain technology for resilient and robust frequency control in a renewable-based hybrid power system with hydrogen and battery storage integration,'' *Energy Convers. Manage.*, vol. 283, May 2023, Art. no. 116888.

[44] Y. Wang, D. Zhang, Y. Li, W. Jiao, G. Wang, J. Zhao, Y. Qiang, and K. Li, ''Enhancing power grid resilience with blockchain-enabled vehicle-to-vehicle energy trading in renewable energy integration,'' *IEEE Trans. Ind. Appl.*, vol. 60, no. 2, pp. 2037–2052, Mar. 2024.

[45] V. Veerasamy, Z. Hu, H. Qiu, S. Murshid, H. B. Gooi, and H. D. Nguyen, ''Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids,'' *Appl. Energy*, vol. 353, Jan. 2024, Art. no. 122107.

SEERIN AHMAD (Graduate Student Member, IEEE) received the B.E. degree in electrical engineering from Aligarh Muslim University, Aligarh, India, in 2017, and the M.S. degree in electrical engineering from Budapest University of Technology and Economics, Budapest, Hungary, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with Texas A&M University–Kingsville, Kingsville, TX, USA. He was also with Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA, in 2024. His research interests include cyber-resilient power systems, distributed energy resource management systems, power electronics, and cybersecurity.

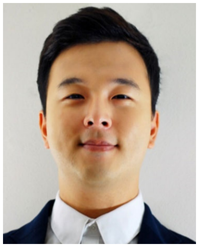
KALYAN NAKKA received the B.Tech. degree in mechanical engineering from Indian Institute of Technology (IIT), Dhanbad, in 2016, and the M.S. degree in computer science from Texas A&M University–Kingsville (TAMUK), in 2023. He is currently pursuing the Ph.D. degree in computer science with Texas A&M University (TAMU). He was a mid-senior-level software engineering professional with five years of experience and worked at various companies in India, from 2016 to 2021. His research interests include deep learning, adversarial machine learning, and AI/ML Security.



TAESIC KIM (Senior Member, IEEE) received the B.S. degree in electronics engineering from Changwon National University, Changwon, South Korea, in 2008, and the M.S. and Ph.D. degrees in electrical engineering and computer engineering from the University of Nebraska–Lincoln, in 2012 and 2015, respectively. In 2009, he was with the New and Renewable Energy Research Group, Korea Electrotechnology Research Institute, South Korea. He was also with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA, in 2013. He was an Associate Professor with the Department of Electrical Engineering and Computer Science, Texas A&M University–Kingsville. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia. His research interests include cyberphysical power and energy systems, including cyber-physical system security, power electronics and cyber-resilient power systems, quantum machine learning and optimization, and blockchain. He was a recipient of the 2018 Myron Zucker Student-Faculty Grant Award from the IEEE Foundation, the Best Paper Awards in the 2021 IEEE PES Innovative Smart Grid Technologies-Asia and the 2017 IEEE International Conference on Electro Information Technology, and the First Prize Award in the 2013 IEEE Industry Application Society Graduate Student Thesis Contest.

DONGJUN HAN (Graduate Student Member, IEEE) was born in Incheon, Republic of Korea, in 1995. He received the B.S. degree in electrical engineering from Inha University, Incheon, in 2021, where he is currently pursuing the integrated M.S. and Ph.D. degrees in electrical engineering. His research interests include power system artificial intelligence application, energy market, distributed energy resource, and active distribution networks.

DONGJUN WON (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2004, respectively. He was a Postdoctoral Fellow with the APT Center, University of Washington, Seattle, and an affiliate with Lawrence Berkeley National Laboratory, Berkeley. Currently, he is a Professor with the School of Electrical Engineering, Inha University, Incheon, South Korea. His research interests include distributed energy resources, microgrids, electric vehicles, and energy storage systems.



BOHYUN AHN (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Minnesota State University-Mankato in 2016 and 2018, respectively, and the Ph.D. degree in engineering (electrical engineering specialization) from Texas A&M University-Kingsville in 2024. He was with the National Renewable Energy Laboratories (NREL), Golden, CO, USA, in 2023. Currently, he is a Post-Doctoral Fellow with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, USA. His current research interests include cyber-secure smart inverter, malware security, ethical hacking, memory forensics, and blockchain-based security. He is a recipient of 1st place in 2022 IEEE ECCE student demo project software competition.