Blockchain-Assisted Cybersecurity for Solar Farm

BoHyun Ahn, *Member, IEEE*, Taesic Kim, *Senior Member, IEEE*, Kalyan Nakka, Jinchun Choi, Seerin Ahmad, *Member, IEEE*, Hee-Yong Kwon, Nathanial R. Handke, and Trevor J. Reyna

***Abstract*—This article explores how blockchain (BC) technologies can improve cybersecurity of photovoltaic (PV) systems, specifically solar farms. First of all, a comprehensive BC-assisted security framework is proposed which has distinct stages: 1) Prevention stage including a solar farm membership service, solar asset management, secure BC data communication, secure boot verification, and self-signed certificate verification; 2) Detection and Incident Response stage including man-in-the-middle (MITM) attack detection, firmware attack detection, alert, and response; and 3) Recovery and Resilience stage including access control, firmware patching and rollback, and resilient control. Moreover, this article introduces a BC-integrated security module (SM) design providing an industry-deployable method of the proposed BC framework in the PV system. This article also provides practical cyberattack models targeting a commercial solar farm with real-world field testing methods. Finally, the testing results demonstrate that the proposed BC-assisted system proactively detects MITM attacks, firmware modification attack, and malware attack, while ensuring the continuous operation of the solar farm during attack events.**

***Index Terms*—Blockchain, cyberattack, cybersecurity, field demo, photovoltaic (PV) system, solar farm, solar inverter.**

I. Introduction

CYBERSECURITY is vital for photovoltaic (PV) systems to ensure the reliable and safe operation of modern power grids. As PV systems become more dominant (e.g., total U.S. electricity to 40% (1000 GWac) by 2035 and further to 45% by 2050 (1600 GWac) [1]) and increasingly reliant on digital technology, their primary application, solar farms, is becoming critical infrastructure, and thus an attractive target for cyberattacks by threat actors. The first cyberattack on U.S. PV systems was reported on March 5, 2019 [2]. A malicious actor repeatedly rebooted sPower's communication devices, causing multiple five-minute communication losses between its control center and 500 MW of solar and wind generation facilities in Utah [2]. In 2022, a threat actor tampered with solar inverter firmware, gaining access to personal data of Dutch customers, creating new profiles, deleting existing accounts, and obtaining electricity generation data using GPS coordinates [3]. In 2023, a flawed vendor software update unintentionally disabled 800 Sungrow PV home storage units [4]. That same year, sensitive data from more than 130000 European-manufactured solar energy monitoring systems were exposed online, potentially enabling unauthorized remote access (i.e., a backdoor) [5]. A separate demonstration showed malicious manipulation of numerous solar inverters from well-known German manufacturers, exploiting vulnerabilities in unsecured firmware updates within cloud-connected PV systems [6]. Since 2012, more than 88 publicly reported cases of cyberattacks and disclosed vulnerabilities in solar systems have been documented, with cases expected to rise further [7]. These real-world incidents and vulnerability reports highlight the urgency of protecting PV systems from evolving cyber threats.

Studies on power system cybersecurity have focused on three main areas: detecting and responding to false data injection attacks (FDIAs) with data-driven learning [8], improving reliability for access control, communication security, and firmware integrity [9], [10], [11], [12], and enhancing the scalability of consensus protocols [13]. In the case of current PV systems, particularly solar farms, they primarily rely on industry security standards (i.e., IEEE 1547.3-2023 [14]) and network-based measures such as user authentication, firewall rules, and encrypted communication using the Transport Layer Security (TLS) protocol [15], [16]. A comprehensive review of solar farm cybersecurity covering firmware, networks, inverter controls, and grid-level considerations—is presented in [17]. In addition, [18] provides an overview of cyber-resilient solar farm inverter design based on fifteen practical attack models. A multi-level cybersecurity framework and field testing for commercially operated solar farms, spanning inverter device-level to system-level protections and incorporating hardware hardening, intrusion detection, and recovery strategies, is discussed in [19]. Cyberattack

Received 15 July 2025; revised 18 September 2025; accepted 19 October 2025. Date of publication 23 December 2025; date of current version 20 July 2026. Paper 2025-SECSC-1265.R1, presented at the 2024 IEEE Energy Conversion Congress and Exposition, Phoenix, AZ, USA, Oct. 20–24, and approved for publication in the IEEE Transactions on Industry Applications by the Renewable and Sustainable Energy Conversion Systems Committee of the IEEE Industry Applications Society [DOI: 10.1109/ECCE55643.2024.10860909]. This work was supported in part by the National Science Foundation (NSF) under Award CNS-2219733 and in part by the U.S. Department of Energy under Grant DE-EE0009026. *(Corresponding author: Taesic Kim.)*

BoHyun Ahn, Taesic Kim, and Hee-Yong Kwon are with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO 65201 USA (e-mail: bapn4@missouri.edu; tkx96@missouri.edu; hktxr@missouri.edu).

Kalyan Nakka is with the Department of Computer Science and Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: kalyan@tamu.edu).

Jinchun Choi is with the Cyber Warfare Technology Research Center, Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea (e-mail: jcchoi@etri.re.kr).

Seerin Ahmad is with the System Performance Analysis Department, American Electric Power(AEP), New Albany, OH 43054 USA (e-mail: sahmad@aep.com).

Nathanial R. Handke and Trevor J. Reyna are with the Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX 78363 USA (e-mail: nathanial.handke@students.tamuk.edu; trevor.reyna@students.tamuk.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIA.2025.3644992.

Digital Object Identifier 10.1109/TIA.2025.3644992

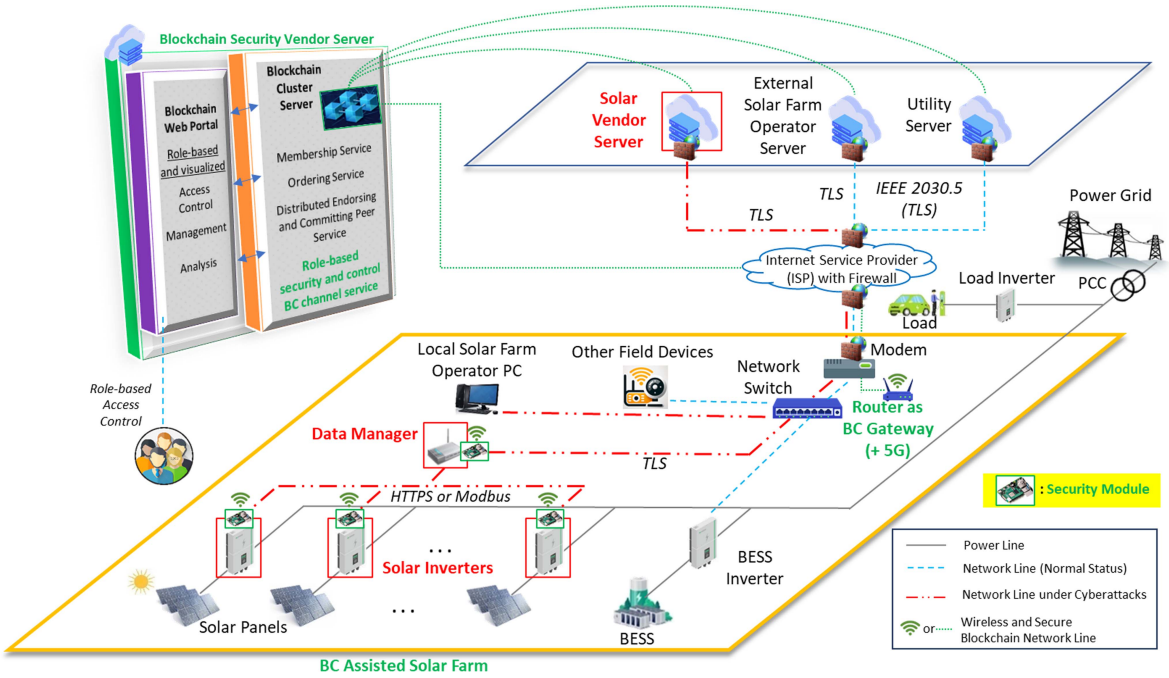

Fig. 1. A solar farm integrating the proposed BC-assisted security framework to protect solar farm operations.

tactics continue to evolve with advances in technologies such as artificial intelligence (AI) and quantum computing, as well as increasing adversarial expertise. However, it remains uncertain whether existing cybersecurity methods can effectively adapt to secure field-deployed, specifically non–utility-owned solar farms.

Beyond existing cybersecurity methods and studies, blockchain (BC) technology offers a broader, more adaptable, and deeper system-level security framework. By leveraging advances in cryptography, public key infrastructure (PKI), consensus mechanisms, and role-based access control, BC can address [20] and mitigate a wide range of real-world existing and emerging attack cases. In particular, the authors investigated and observed that current commercial solar inverter products typically rely on self-signed certificates to communicate with client devices, without adequately addressing the associated security risks. In contrast, the proposed BC framework enables certificate validation through event-driven integrity checking.

This article is extended works of [21] and detailed system-level BC-assisted security work of [19] to provide a holistic view of BC-assisted security framework for solar farms. This article also provides a comprehensive attack modeling method, industry-deployable BC-assisted security implementation method using security modules (SMs), and more detailed solar farm field demo testing methods and results.

The main contributions of this article are given as follows:

1) Developed a holistic BC-assisted security framework to enhance security level of solar farms.
2) Created a BC-enabled SM prototype for seamless deployment and adaptable integration in solar farms.
3) Developed BC-assisted data verification method enabling to verify critical data such as external control commands, new firmware files, secure boot public keys, and self-signed certificates stored in real-world commercial solar inverter products.
4) Developed a BC-enabled SM prototype for seamless BC and security feature deployment in legacy solar farms or solar farms with less security features.
5) Provided detailed cyberattack models with field testing methods for solar farms.
6) Established a foundational reference to help solar farm cybersecurity teams adopt security-by-design principles.
7) Released an open-source BC security reference code with supporting implementation and demonstration videos.

II. Related Works

A. A Solar Farm System Identification

Fig. 1 depicts an example of a solar farm. The solar farm comprises multiple string solar inverters (i.e., a fleet of solar inverters) linked to a data manager (i.e., inverter aggregator and gateway), a battery energy storage system (BESS) with its inverter, solar farm network devices (such as router, network switch, and modem), a local operator PC, and other field devices. The local operator PC as a Human-Machine Interface (HMI) enables centralized management of solar farm devices. Solar inverters (also referred to as smart inverters) are the 'brain and heart' of a solar farm. They not only enable power conversion but also remotely manage solar generation and grid supports, either independently or in coordination with the data manager [18]. As such, they are critical cyber-physical solar assets that must be protected against evolving cyberattacks.

Fig. 1 illustrates multiple connections: 1) the power line (black solid), 2) the network line under normal operation (blue dotted), 3) the network line under cyberattack (red long dash-dot), and 4) the wireless and secure BC network line (green, represented by

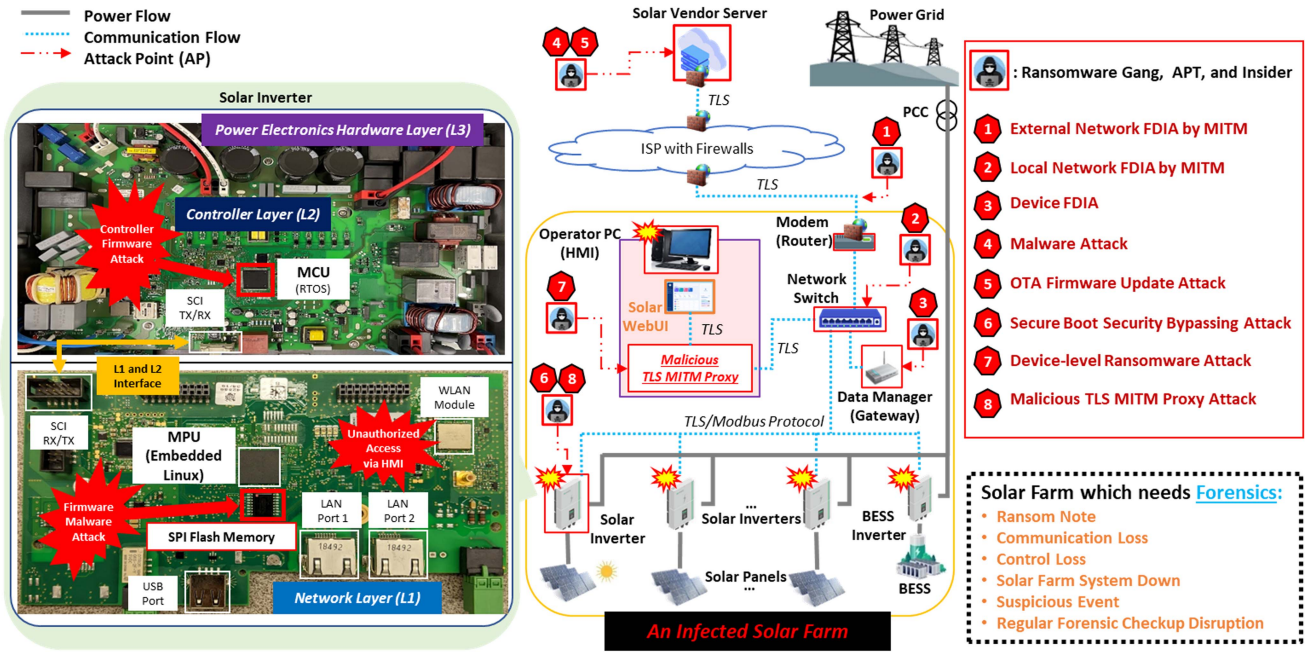

Fig. 2. Attack surface of the solar farm to be mitigated by the proposed BC framework.

a Wi-Fi symbol or round dash). While additional attack vectors may exist (such as those between the utility server and the target solar farm), this article only focuses on attack scenarios specific to a non–utility-owned solar farm (i.e., third-party owned solar farm). More detailed attack types and vectors for this solar farm are presented in Fig. 2.

Each solar farm device typically supports connectivity and communication through standard network protocols defined in IEEE 1547-2023 (e.g., SunSpec Modbus, DNP3, and IEEE 2030.5) as well as proprietary protocols such as HTTPS (HTTP+TLS) [14]. However, these protocols still contain unresolved vulnerabilities and remain susceptible to man-in-the-middle (MITM) and denial-of-service (DOS) attacks [18]. To address this, a security module (SM) is passively integrated into each solar farm device, enabling access to the additional secure BC network line. This line operates independently, remaining isolated from cyberattacks on the conventional network and avoiding disruption to existing remote solar farm operations. Devices communicate wirelessly with a BC security vendor server via a router that functions as a BC gateway, for example, using a 5G network. The BC security vendor server includes: 1) a main BC cluster server, which provides membership services, ordering services, distributed endorsing and committing peer services, as well as role-based security and BC channel control; and 2) a role-based and visualized BC web portal that allows authorized solar farm BC participants to manage access, monitor performance, and perform security analysis.

B. Attack Surface of a Solar Farm

An example of commercial solar inverter product is structured into three essential layers [18], depicted in Fig. 2: 1) Network Layer (*L1*), 2) Controller Layer (*L2*), and 3) Power Electronics Hardware Layer (*L3*). At *L1*, a microprocessor unit (MPU) with ARM architecture stores a read-only memory (ROM) first stage bootloader (e.g., MLO). This layer also incorporates a serial peripheral interface (SPI) flash memory for storing second stage bootloaders (e.g., Barebox, U-Boot), kernel, and root file systems, along with various peripheral network components like LAN ports, a Wi-Fi module, USB, a serial communication interface (SCI) module, and a Joint Test Action Group (JTAG) debugging port. The *L1* functions like a typical IoT edge device, allowing secure and direct connection to external network servers through TLS version 1.2/1.3 protocol. Users and installers can directly access the solar inverters through a locally hosted web user interface (WebUI) through local or cloud-based access via the inverter data manager over the public Internet. The *L2* has a microcontroller unit (MCU) providing lightweight computing power for signal processing and inverter control. An internal MCU memory hosts a real-time operating system (RTOS) for controller firmware, which can be updated through *L1* in *L2*. The *L3* encompasses power electronics hardware components such as power switches, gate drives, relays, analog filters, sensors, and serial communication interfaces, establishing connections with *L2*.

Based on the solar farm model (from the non-utility-owned solar vendor server to the solar farm) indicated in Fig. 1, a total of eight attack surfaces, or attack points (*AP*s), are identified in Fig. 2. Potential adversaries include ransomware gangs (financial gaining purposed organizations through encrypting data and demanding payment for its decryption), Advanced Persistent Threat (APT) groups (state-sponsored or well-resourced organizations that engage in long-term, stealthy cyberespionage, often targeting specific critical system for intelligence gathering), and insiders. An external network FDIA can occur between the solar vendor server and the solar farm (*AP1*) if a MITM proxy server

Fig. 3. Current certificate technology deployed in a commercial solar product.

exploits a PKI and self-signed certificate (a currently deployed certificate method in commercial solar products as depicted in Fig. 3.) vulnerabilities in TLS. Additionally, an unauthorized device connected to the network switch can conduct a local network FDIA via an MITM device (*AP2*). In addition, a device-level FDIA (*AP3*) can take place if the data manager is compromised through a malicious firmware update. If the vendor server's codesigning key is leaked, it can be used to generate malware (*AP4*) or create a malicious firmware update (*AP5*) targeting the solar inverter. Furthermore, extracting the public keys stored in the solar inverter could allow an attacker to bypass secure boot protections (*AP6*).

Traditionally, external solar farm operators and utilities access inverters remotely through the local operator's PC. However, external vendors can also access multiple inverters remotely via a cloud-connected solar WebUI over HTTP/HTTPS through the data manager. This WebUI enables monitoring of inverter status, solar energy production, and adjustments to settings, control parameters, and firmware updates. Despite its convenience, this direct access method presents a critical attack point. If inverters connected to the data manager are compromised (*AP7*), overall solar farm operations could be disrupted [22]. Finally, a device-level ransomware attack could encrypt critical system configuration files, preventing remote access by authorized users (*AP8*) [23].

Each defined attack, occurring at specific locations, can generate attack evidence such as ransom notes, communication or control loss, system downtime, suspicious activities, and disruptions to regular forensic checkups. This information can be used to identify the attack type and location after it occurs. However, by using the proposed BC-assisted framework with integrated security modules (SMs) that communicate with the BC cluster server and BC web portal, as illustrated in Fig. 1, the eight attacks can be proactively mitigated in real time.

C. An Example of Practical Attack Models Targeting a Solar Farm

Based on the *APs* described in Section II-B, a solar farm attack model was designed by integrating historical cases of real-world solar energy cyberattacks and vulnerabilities [7] with the MITRE ATT&CK ICS framework [24]. The model assumes an adversary who obtains WebUI credentials, accesses the WebUI, and compromises multiple inverters through malicious configuration changes and firmware updates to disrupt operations as follows:

1) Access the cloud-connected solar WebUI of the data manager using maliciously acquired remote credentials, exploiting missing cloud API authorization.
2) Conduct reconnaissance within the solar WebUI environment of the data manager to identify additional network vulnerabilities (e.g., poorly segmented VPN networks).
3) Establish or elevate privileges to a Super Administrator account to ensure persistence and evade detection.
4) Discover and gain access to all connected solar inverters (The report [7] introduced a case about the ability to access 10000 solar devices).
5) Collect information about target inverter configuration settings and the current firmware version.
6) Tamper with configuration settings (e.g., disabling grid-support functions) on the solar inverters.
7) Upload malicious firmware (exploiting vulnerabilities such as missing code signing and secure boot) to the MPU of L1 to disrupt authorized network operation and monitoring.
8) Retrieve the controller-related firmware binary to the MCU (*L2*) to impair all solar inverter control functions.
9) Render the entire solar farm operation non-functional (The report [7] introduced a case about the ability to brick 10000 solar devices).

The attack model (G) can be represented as a directed acyclic graph (DAG) [25],

$$G = (V, E)$$

where vertices (V) denote system states and edges (E) denote exploit-driven transitions. The attack begins at

v_0 (stable operation) and progresses forward through:

v_1(WebUI access), v_2(reconnaissance), v_3 (privilege escalation, v_4(persistence), v_5(detection evasion), v_6 (inverters discovered), v_7 (inverter information collected), v_8 (configurations tampered), v_9 (malicious firmware uploaded to MPU (*L1*)), v_{10} (firmware deployed to MCU (*L2*)), terminating in v_{11}(solar farm non-functional). Either branching edges (e.g., $e_{2\to3}, e_{2\to4}, e_{2\to5}$) or sequential edges (e.g., $e_{8\to9}, e_{9\to10}, e_{10\to11}$) are available for the successful attack. Optional edge weights $w(e) \in [0,\ 1]$ can be added by exploitation risk or probability such as derived from CVSS scores [26].

The Overall Attack Success Probability Along a Path is

$$P\ (G) = \prod_{e \in path} p\,(e)$$

with $|V| =$ 12 and $|E| \approx 12$, the graph can allow efficient traversal $O(|V| + |E|)$time.

III. An Overview of BC-Assisted Security Framework and Model for a Solar Farm

A. Holistic BC-assisted Security Framework

The BC-assisted security framework depicted in Fig. 4. includes essential cybersecurity components. This framework is composed of three security stages: 1) prevention, 2) detection

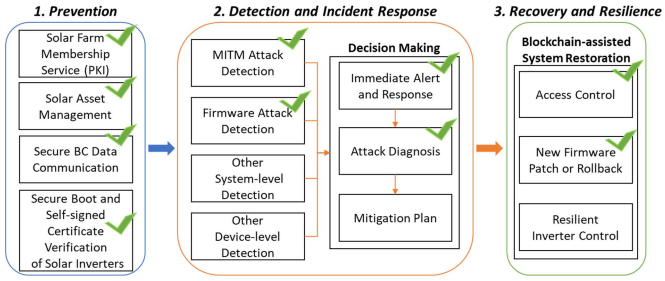

Fig. 4. BC-assisted security framework for a solar farm.

and incident response, and 3) recovery and resilience. The green-colored check marks have been achieved and validated in this research.

The prevention stage includes a membership service that functions as a PKI within the Hyperledger Fabric (HLF) BC platform used in this research. An BC audit trail is maintained to track and monitor the status of solar devices at grid edge and their critical data. BC data is also securely transmitted through the establishment of the TLS version 1.3 protocol. Therefore, with secure transmission and data integrity ensured, critical information recorded on the distributed BC ledger can be tracked securely, enhancing situational awareness. In addition, whenever the solar inverter system boots, its bootloader firmware and self-signed certificate is automatically verified by the BC to ensure secure booting and inverter device (server) authenticity. In the detection and the incident response stage, all incoming and outgoing control command data, along with new firmware files, are cryptographically verified and signed by the sender, ensuring authentication and data integrity within the BC network. This process enables the detection of MITM and firmware attacks, triggering immediate alerts and responses with attack diagnostics. The distributed architecture of BC ledgers mitigates the risk of a single point of failure caused by potential data tampering risks. In the recovery and resilience stage, BC smart contract-based access control securely adjusts inverter settings and control parameters to restore the solar inverter. BC also enables secure firmware updates and rollbacks to restore solar inverters. Additionally, by activating a control channel for the solar farm during network outages caused by DOS attacks, functionality is rapidly restored through the integration of resilient inverter controls.

B. BC Model

Fig. 5. illustrates a solar farm-tailored BC model. By leveraging the private BC features, a more collaborative security ecosystem can be established, allowing multiple parties (e.g., solar vendors, solar farm operators, and utilities) to efficiently handle user- or vendor-identified incidents through effective notification, coordination, disclosure, and validation mechanisms while safeguarding the privacy of the solar farm using smart contracts and a multichannel BC. The multichannel platform adopts a modular architecture where client/peer nodes can be hosted on a party's server or cloud system, leveraging parallelism by assigning a unique ordering and a fast peer server per channel. This BC model is designed to operate under a zero-trust security

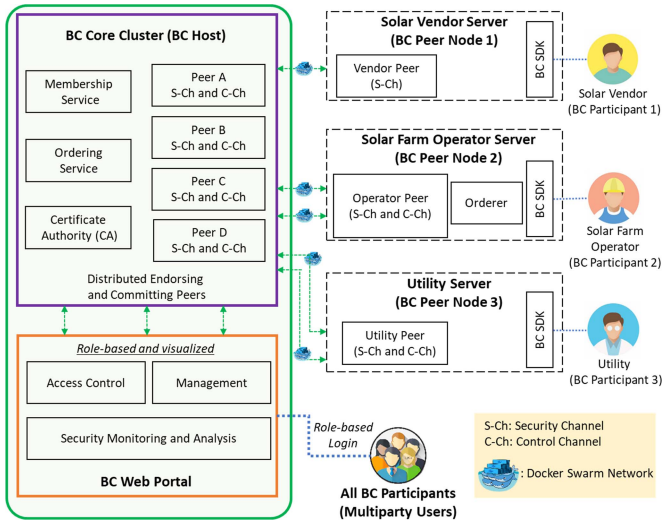

Fig. 5. Solar farm-tailored BC model.

model. By consistently and continuously verifying identity, validating activities, and limiting access and privileges, the security services of the system can be trusted, ensuring the integrity and authenticity of critical assets and providing a practical solution to manage the emerging cyber risks associated with the solar farm.

The integration of BC technology has the potential to enhance the security of third-party vendor-owned solar farms by evaluating and securing endpoint solar devices, such as solar inverters and data managers, which function as BC client nodes. These nodes collaborate with other authorized BC peer nodes (who are already joined BC private network, e.g., local solar farm operator PCs, solar vendor servers, external solar operator servers, and utility servers) within the same BC network to validate shared data. An authorized BC core cluster securely manages all BC participant nodes through a private membership service within a distributed and integrated BC ledger. This cluster also enables secure communication via dedicated BC channels, such as a security BC channel, a command BC channel, or both, depending on the participants assigned roles. The BC core cluster also includes an integrated web portal program that provides role-based, visualized access control, asset management, and real-time analysis. Through this web portal, all BC participants can directly monitor and manage solar devices using role-specific accounts, enabling intuitive and efficient oversight.

C. BC-assisted Data Verification Method

Fig. 6. illustrates a case study of the BC-assisted data verification method for validating new control commands or firmware updates against complex and multi-vector cyberattacks.

1) *Prevention:* The solar vendor server (i.e., BC Client Node 1), data manager SM (i.e., BC Client Node 2), and solar inverter SM (i.e., BC Client Node 3) operate as BC client nodes within the same BC network channel. When the solar vendor server prepares a target data payload, it signs the data using its private key. Prior to transmission, the server reports a new transaction (TX#1) to the data

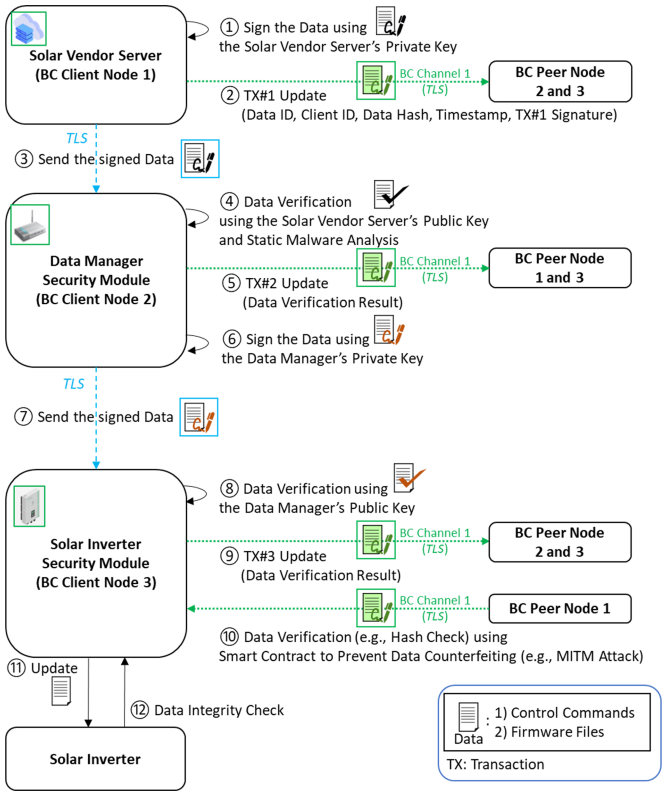

Fig. 6. BC-assisted data verification workflow.

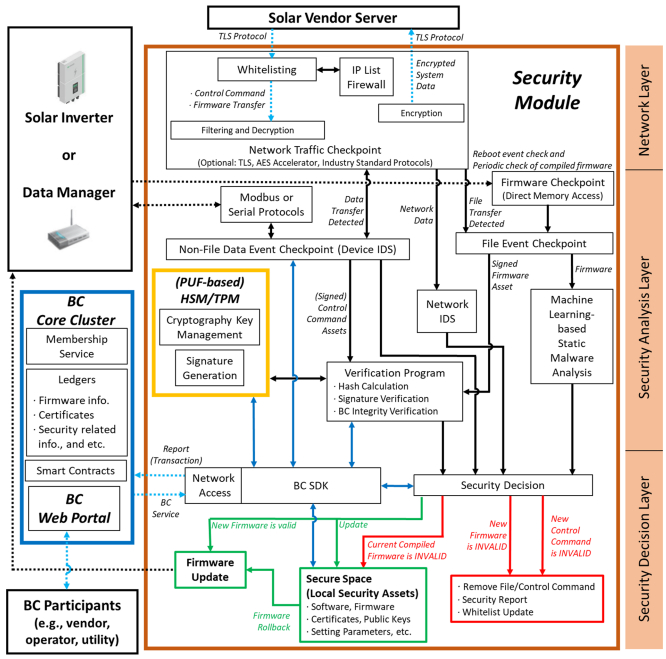

Fig. 7. SM reference design.

manager and solar inverter BC nodes, containing the target data ID, data hash, solar vendor ID, timestamp, and TX#1 signature.

2) *Dectection and Incident Response:* Upon receiving the signed data, the data manager SM verifies it using the solar vendor server's public key. If the data is a firmware payload, it undergoes malware detection process (e.g., static malware analysis). After verification, the result is reported to solar vendor and solar inverter BC nodes. If it fails, the corresponding attack result will be reported to the BC nodes, and the forwarding update process will be automatically halted. The data manager SM then signs the data with its own private key. Next, the solar inverter SM receives the data from the data manager SM and verifies it using the data manager's public key. The inverter then updates the verification result to the solar vendor and data manager BC nodes. To defend against MITM attacks, the inverter performs additional hash-based verification using a smart contract and compares it with the original data hash stored by the solar vendor BC node. If all checks are passed, the solar inverter security module delivers the verified data to the inverter device's lower layers (*L2+L3*) for application. However, if not, this update process will be automatically suspended. A final integrity check is performed internally between the inverter (*L2+L3*) and the security module (*L1*), using an embedded security program.

3) *Recovery and Resilience:* If BC nodes detect any undefined or uncertain activity via cyberattacks, remedial actions such as micro-patching through inverter parameter correction, deploying a new firmware patch or rollback, or initiating resilient inverter control can be applied.

IV. SM Development for Supporting Security Features

To enable the integration of conventional solar inverters and the data manager with the BC network, a SM has been specifically designed and developed to ensure seamless interfacing, as illustrated in Fig. 7. This design provides security functions for both 1) the network board of the solar inverter (*L1*), with minimized and optimized security features, and 2) the data manager, which is fully equipped with security functions as a BC-enabled secure gateway device. The designed SM also enhances the security of both solar device types, addressing the limitations of commercially available solar products that lack support for advanced security functions and BC interface programs. From the industry-deployable perspective that avoids disrupting original operations, two solar inverter vendor products [27] and [28] were tested. Both products support Ethernet and Wi-Fi connectivity for conventional operation interfaces with their corresponding embedded HTTPS web server (uses self-signed certificate), but they were successfully integrated with the developed SMs via a reverse HTTPS proxy [29] without requiring any product-side modifications.

The use of static malware analysis, which initially relied on an external malware scanning service (e.g., VirusTotal) and the open-source tool, PeFrame, to extract static features from files—such as hashes, URLs, and IP addresses. However, this method depends on the conventional network line described in Fig. 1 for internet access and is limited to detecting only known or previously reported malware. Furthermore, it becomes unavailable during periods of unstable conventional network line connectivity, such as during a DOS attack. To overcome

TABLE I
DESIGNED TEST CASES

Test Case (TC)	Attack Type	Vulnerability	Attack Vector (Way of Attack)	Description (Penetration Testing)	Goal of Attack
TC-1	External Network FDIA by MITM	1) PKI Vulnerability in TLS (CVE-2015-8960) 2) Improper Certificate Validation (CVE-2025-8393)	1) A stolen TLS certificate key, 2) A maliciously exploited TLS CA could create external MITM attacks to generate a FDIA, or 3) Security vulnerabilities of self-signed certificates in embedded web servers of data managers and inverters	An unidentified MITM proxy server compromises external control commands between vendor server and data manager, skipping TLS certificate checking	Target solar inverters are off or disrupted by available control commands.
TC-2	Local Network FDIA by MITM	Insecure Local Network Protocol (CVE-2017-9856)	An unauthorized device is physically connected to the network switch on the solar farm then create local MITM attacks a generate a FDIA.	A malicious device performs 1) port scanning, 2) packet sniffing, and 3) tampering a designated control command between data manager and inverter network device.	
TC-3	Device FDIA	Insecure Field Device (CVE-2017-9860)	Through a malicious firmware update, the data manager is compromised, which enables the opening of a backdoor port. Consequently, the device is transformed into a MITM device capable of generating a FDIA.	The attacker gains access to data manager and proceeds to tamper with a control command-related program, compromising the connection between data manager and inverter network device.	
TC-4	Malware Attack	Insecure Vendor's Codesigning System (CVE-2020-0601)	The attacker steals the vendor's codesigning key, then uses it to sign malware.	Compromised vendor server sends malware to the solar farm and data manager receives it first.	Trojan malware on the solar inverters is used to disrupt their normal operations.
TC-5	OTA Firmware Update Attack	Insecure Vendor's Codesigning System (CVE-2020-0601)	The attacker steals the vendor's codesigning key, and then utilizes it to sign a malicious firmware for the inverter controller.	Compromised vendor server sends a malicious firmware for the inverter controller to the solar farm and data manager receives it first.	The controller firmware that has been tampered with maliciously creates a sensor DIA.
TC-6	Secure Boot Security Bypassing Attack	Insecure Field Device (CVE-2023-20082; CVE-2024-39584)	The attacker maliciously extracts the public key used for Secure Boot image signature verification from the SPI flash memory of an affected solar inverter.	An authenticated local attacker with a certain privileges, or an unauthenticated intruder physically accesses to the SPI flash memory of the solar inverter.	The attacker bypasses the secure boot of the compromised solar inverter and executes persistent code to disrupt OS system.

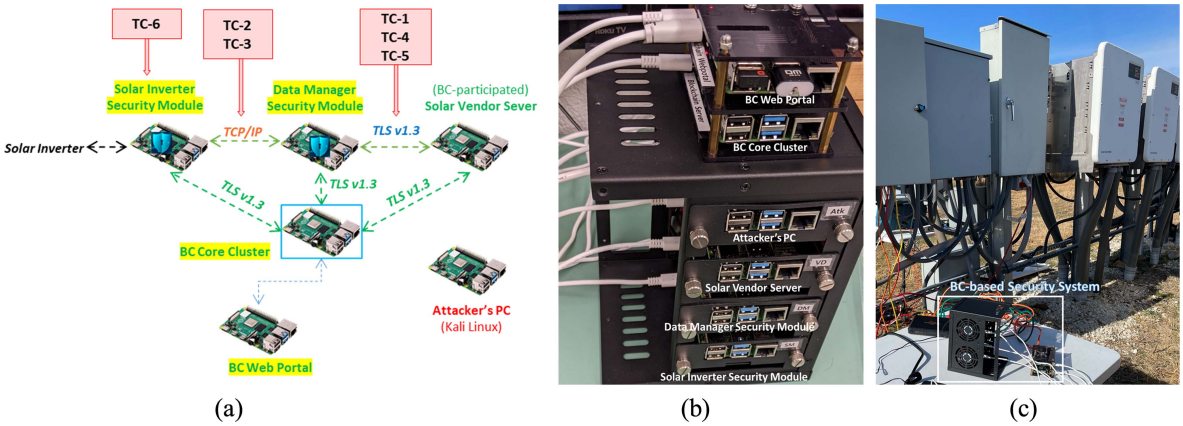

Fig. 8. BC-assisted security system for TCs: (a) system configuration, (b) system hardware, and (c) system deployment in a commercial solar farm.

these limitations, a device-centric, machine learning (ML)–based static malware analysis approach [30] was developed and integrated into the latest version of the SM.

The SM and BC core cluster collaborate to verify the integrity of control commands and firmware while they are in transit by checking their hash values using a BC smart contract program. As a result, this BC-interfaced SM is capable of detecting MITM-based FDIAs, malicious firmware attacks, inverter bootloader firmware tampering, and inverter recovery, while ensuring the integrity of in-transit or stored ledger data in real-time. Overall, this comprehensive SM design ensures secure communication between all assets and the BC core cluster using the TLS protocol via conceptually a secure BC network line that is isolated from the conventional solar farm network.

V. TESTING DESIGN AN EXPERIMENTAL SETUP

A. Testing Design

Through a combination of literature search, input from industry partners [19], and recent attack incident reports, as well as vulnerability analysis, security risks for solar farm were identified. Based on this analysis, potential attack vectors were also defined and six test cases (*TC*s) focused on first six *AP*s addressed in Section II-B. A complete list of these TCs can be found in Table I. *TC-1*, *TC-2*, and *TC-3* are related to control command attacks involving MITM-based FDIAs, while *TC-4* and *TC-5* are related to firmware update-related attacks involving malware or maliciously tampered firmware provided by compromised vendors. *TC-6* is an embedded firmware attack through malicious physical access to the solar inverter board, supply chain breaches, or firmware update attacks.

B. Experimental Setup

Fig. 8 illustrates the developed BC-assisted security system used for conducting the BC-assisted defense demonstrations against the devised TC attacks in the commercial solar farm. This system allows the solar farm operators to easily set up and test cyberattacks, i.e., plug and play for their solar farm system. Fig. 8(a) shows the hardware setup of the BC-assisted

```
pi@datamanager:~/Desktop/test_bed_2/data_manager $ sudo python3 tc4_data_manager.py

Waiting for Connection (from Security Module)

Successfully Connected to Security Module ('192.168.1.133', 7777)

Waiting for Connection (from Vendor)

Successfully Connected to Vendor ('192.168.1.119', 33688)
\Control command from Vendor: firmware_malware.bin;MEUCIQDdXPxpbaFYTuQGi2cXNj6ZvtMR/NxkHcmFgLSq01cFsQIgNRsV7Vw1h9W/IYH405yOk/QtaqmZrjilbB650qOFmQk=;Firmware_ID_6404559
1/1 [==============================] - 1s 705ms/step

Firmware binary file is verified as a Malware

The received firmware binary file is verified as a Malware by ML

status code: 200
Firmware data from Blockchain for the data integrity check

recv: {'FileType': 'Firmware', 'Name': 'UCB_01', 'Version': '2.0.0', 'Hash': '9d47a51c54b3cbaf4ef67acb15c9d198a9af110ebf213c9f45248bf61ce78b97', 'Owned': 'Vendor', 'Status':
 'Normal', 'Time_Stamp': '10/05/2023 13:20:21'}

status code: 200
Malware is updated to the Blockchain
```

Fig. 9. TC-4 detection and response results (SM screen via BC SDK).

security system, highlighting each TC experiment point for the field testing. The hardware is set up, comprising six Raspberry Pis representing distinct components: the solar inverter SM, the data manager SM, the solar vendor server, the attacker's PC, the BC core cluster, and the BC web portal. It is assumed that the solar vendor server is positioned externally outside of the solar farm, hence emulating the use of the TLS version 1.3 protocol for communication with the data manager. The TCP/IP protocol is employed between the solar inverter and the data manager to emulate Modbus TCP/IP protocol. Moreover, TLS version 1.3 protocol is utilized for securely encrypted communication between the BC client/peer nodes and the BC core cluster.

Compared to the earlier BC-assisted security system introduced in [20], which required multiple PCs/laptops with different OSs mixed with IoT devices, the current system presented in this paper has been developed using only 64-bit ARM processor-based, low-cost Raspberry Pi 4B devices. This was made possible by HLF version 2.5's official support for ARM processors since early 2023. Additionally, the optimized and device-centric lightweight ML algorithm for malware detection, developed in [30], was successfully implemented on the Raspberry Pi 4B. Therefore, Fig. 8(b) illustrates the enhanced hardware system built with a Raspberry Pi 4B stack. This system is then seamlessly integrated into the commercial solar farm for attack-and-defense demonstration purposes, as shown in Fig. 8(c).

VI. Experimental Validation

A. Experimental Validation for TC-4

Fig. 9 shows the results of malware detection (*TC-4*) by the data manager SM. Following the testing description in Table I and testing point in Fig. 8(a), the data manager SM received a new firmware update from the compromised vendor server, which was automatically executed to a verification process through ML. The verification result of the new firmware was classified as malware. Additionally, the data manager SM performed integrity and authentication checks against the firmware with records previously stored in the ledger from the compromised vendor. Finally, all verification outcomes were subsequently updated to the ledger of the BC core cluster. Fig. 10 displays the intuitive result of this malware attack on the BC web portal screen. The screen indicates that the attempted firmware update was identified as malware by the data manager SM, with integrity and authentication checks failing, and includes a timestamp for verification.

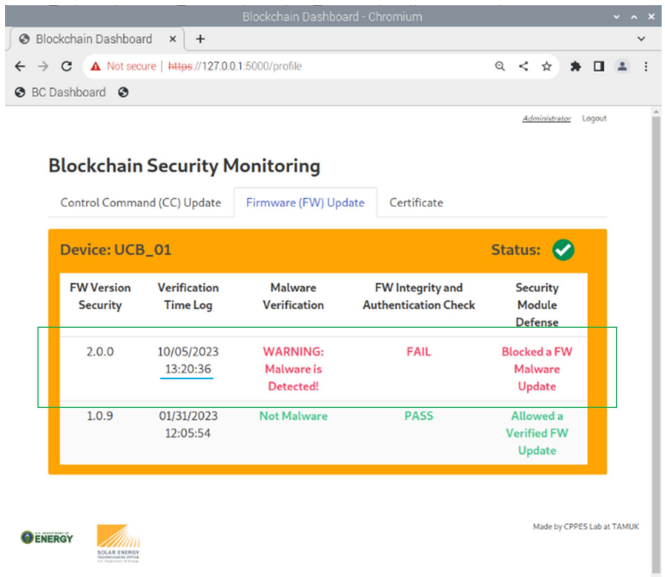

Fig. 10. TC-4 detection and response results (BC web portal screen).

For dataset generation, a benign firmware image stored in the SPI flash memory of *L1* in the commercial solar inverter was extracted. From this, 100 benign variants and 100 malicious variants were generated using binary modifications, with the data split evenly for training (50%) and validation (50%). This approach initially employs a convolutional neural network (CNN) model that analyzes 2D grayscale images converted from binary files. Subsequently, a deep transfer learning (DTL) method [31] was applied by utilizing a pre-trained image recognition model—freezing a subset of layers and finetuning the remaining layers using the new malware dataset. The small dataset was sufficient to achieve higher accuracy and faster convergence by adopting the DTL method. It is noted that the target malware (i.e., Moonbounce bootkit) used in this study was a publicly disclosed sample [32], employed to verify the feasibility of the proposed BC method, while unseen emerging malware detection

```
pi@securitymodule:~/Desktop/test_bed_3/security_module $ python cert.py

Target Certificate: certificate.crt
Signature Algorithm: RSA-with-SHA256
Result: Success
Valid After: 2025-09-15 11:16:32.998442
Valid Before: 2026-09-15 11:16:32.998442

recv: {'certificate_ID': 'certificate_1', 'TargetCertificate': 'certificate.crt', 'SignatureAlgorithm': 'RSA-with-SHA256', 'Res
ult': 'Success', 'ValidAfter': '2025-09-15 11:16:32.998442', 'ValidBefore': '2026-09-15 11:16:32.998442'}
```

Fig. 11. Automatic self-signed certificate integrity check results (SM screen via BC SDK).

was beyond the scope of this research. For testing in the SM, one benign firmware file and four malware variants were used as input samples for the DTL model. The resulting training accuracy reached 99% , and the validation accuracy was 98% .

The average duration for this defense test was 15 seconds (including 1.705 seconds for processing time using the malware detection by the device-centric ML in the data manager SM) with 100% accuracy. Consequently, the data manager SM effectively prevented the malware update to the solar inverter, ensuring its continuous operation.

B. Experimental Validation for BC-assisted Chain of Trust for Self-signed Certificate Integrity

As shown in Fig. 3 and the reverse engineering of products [27] and [28], it was observed that current commercial solar inverters and data managers host embedded web servers using self-signed certificates. However, they remain vulnerable to MITM attacks due to the lack of a chain of trust. To address this issue, the proposed SM-enabled BC method was employed as a secure trust certification authority (CA). An initially issued valid self-signed certificate from the solar inverter was enrolled into the BC ledger via the SM. Upon every inverter reboot or completion of a firmware update, the certificate stored in the BC ledger is compared against the newly retrieved certificate (which could potentially be compromised inside of the inverter) for automatic integrity verification. If the certificate is invalid, the SM promptly alerts the security team for a potential inverter firmware rollback.

Fig. 11 shows the testing results in the inverter SM. The inverter's self-signed certificate, created using Rivest–Shamir–Adleman (RSA) algorithm with Secure Hash Algorithm-256 (SHA-256), was successfully verified against the BC-enrolled certificate. The verification result is also intuitively displayed on the BC web portal screen. Fig. 12 illustrates automatic self-signed certificate integrity check results (BC in the web portal screen.

C. Overall Experiment Summary and Discussion

Table II summarizes the TC experimental results. To validate the proposed testing, initial experiments were conducted in the university lab. Subsequently, the first five TCs were evaluated at the National Center for Reliable Electric Power Transmission (NCREPT) at the University of Arkansas and in the commercial solar farm for final field testing. The lab environment tests were completed successfully without any issues. However, during the NCREPT evaluation, TC-4 initially failed due to campus

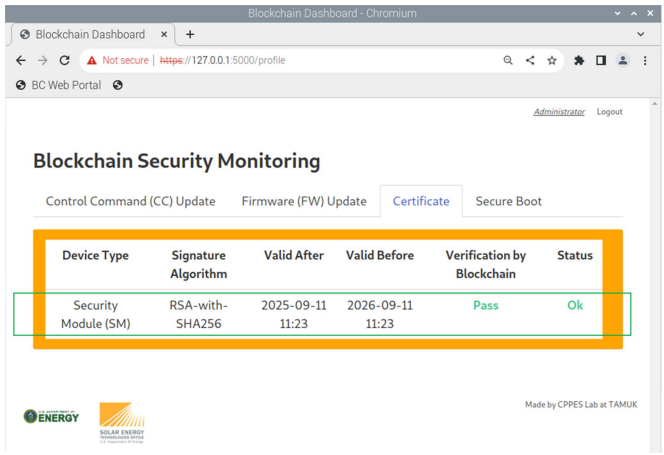

Fig. 12. Automatic self-signed certificate integrity check results (BC web portal screen).

TABLE II
SUMMARY OF TEST CASE EXPERIMENT RESULTS

Test Case (TC)	Attack Type	Average Defense Time (sec)	Univ. Lab Test	Center Test	Solar Farm Test
TC-1	External Network FDIA by MITM	7	O	O	O
TC-2	Local Network FDIA by MITM	13	O	O	O
TC-3	Device FDIA	11	O	O	O
TC-4	Malware Attack	15	O	O	X
TC-5	OTA Firmware Update Attack	18	O	O	X
TC-6	Secure Boot Security Bypassing Attack	4	O	X	X

firewall filtering, which was triggered by the presence of the word '*malware*' in a testing file name. To overcome this obstacle and complete the test, the term was modified to '*m_alware*' to bypass the security filter. In the field tests, TC-1, TC-2, and TC-3 were executed successfully, whereas TC-4 and TC-5 failed due to commercial operator's network security restrictions that

blocked file transfers within the solar farm. No further attempts were made to bypass the field network security in order to preserve operational integrity and avoid disrupting other teams' activities.

The average defense time across all six tests was under 20 seconds, achieving 100% defense accuracy against the corresponding TC attack scenarios. Tests involving control command updates (*TC-1* to *3*) were completed relatively quickly due to the smaller network packet size requirement, while malware/firmware update-related tests (*TC-4* to *5*). Also, *TC-1* to *5* required more time as they involved validation across multiple BC client/peer nodes. The secure boot test (*TC-6*) demonstrated the fastest defense time, as the verified secure boot image in the solar inverter SM was directly validated with the BC core cluster.

One challenge is that the control command execution and firmware update times are slightly longer than usual due to the added defense processing. However, this required processing time effectively enhances the overall security of the PV system, protecting from the inverter device to the server against six types of cyberattacks. Moreover, in the event of an attack, security personnel can intuitively identify the attack point through the BC smart contract, which also facilitates digital forensics in worst-case attack cases. To the best of the author's knowledge, the defense processing time could be further reduced by using an advanced SM device model (e.g., Raspberry Pi 5) equipped with more RAM and an operating system installed on a solid-state drive (SSD). However, these enhancements would also lead to increased system costs. If the SM devices were to be purchased and passively integrated into a fleet of solar inverters through the reverse proxy method—without necessarily degrading the operational performance of large-scale solar farms—it is possible that the estimated costs might be lower than the potential grid risks and power outages that could result from simultaneously halted inverter operations with significant recovering time. Additionally, an optimized BC system from a newly released version or ML libraries may further decrease the defense processing time.

The BC-assisted SM defense mechanism successfully implemented end-to-end solar farm system to ensure continued solar inverter operation during cyberattack events to effectively minimize operation downtime. Additionally, the developed BC prototype module was effectively developed as a plug-and-play hardware solution, allowing for easy deployment in any existing commercial solar farms.

VII. Conclusion

To improve the security of PV systems, this paper introduced BC technology alongside the development of SM. This approach has undergone validation, progressing from field-scale experiments to practical tests in a commercial solar farm, pursuing real-world feasibility. Through a series of cyberattack-and-defense experiments, crucial security features were developed, including defenses against data-modification MITM update attacks, protections against device malware, automatic secure boot, and self-signed certificate verification, all aimed at ensuring the secure operation of the solar inverter. Additionally, the practical BC-assisted security monitoring system accessible via the BC web portal has been developed, providing intuitive insights into cyberattack and defense outcomes, as well as the status of PV system assets throughout operation. Future work includes developing a post-quantum cryptography-enabled BC model to strengthen PV systems against emerging cyber threats in the quantum computing era.

Appendix

Open-source code for a BC security reference code is available on the following GitHub repository [33]. Implementation details and demonstration videos are also provided.

Acknowledgment

This research was conducted while Jinchun Choi was affiliated with Texas A&M University-Kingsville.

References

[1] K. Ardain et al., "Solar futures study," U.S. Department of Energy, Tech. Rep. GO-102021-5621, Sep. 2021.

[2] S. Lyngaas, "Utah renewables company was hit by rare cyberattack in march," CYBERSCOOP, Oct. 2019. [Online]. Available: https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/

[3] E. Bellini, "Dutch agency investigates cybersecurity of pv inverters after hack," Sep. 2022. [Online]. Available: https://www.pv-magazine.com/2022/09/06/dutch-agency-investigates-cybersecurity-of-pv-inverters-after-hack/

[4] S. Enkhardt, "SunGrow: Storage problem will be resolved in a timely manner," Apr. 2023. [Online]. Available: https://www.pv-magazine.com/2023/03/17/around-800-sungrow-batteries-affected-by-outage-in-Germany/

[5] B. Toulas, "Over 130,000 solar energy monitoring systems exposed online," Jul. 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/

[6] Sebastien, "Decentralized energy production: Green future or cybersecurity nightmare?," Dec. 2023. [Online]. Available: https://media.ccc.de/v/37c3-11810-decentralized_energy_production_green_future_or_cybersecurity_nightmare/

[7] J. Johnson, "Public history of solar energy cyberattacks and vulnerabilities," DER Security Corp, DERSEC-SOLAR-VULNS-2.0, May 2025. [Online]. Available: https://dersec.io/reports/DERSec-Solar-Vulnerability-Summary-v2.0-Final.pdf

[8] O. A. Lawal, J. Teh, B. Alharbi, and C.-M. Lai, "Data-driven learning-based classification model for mitigating false data injection attacks on dynamic line rating systems," *Sustain. Energy, Grids Netw.*, vol. 38, 2024, Art. no. 101347.

[9] O. A. Lawal and J. Teh, "A framework for modelling the reliability of dynamic line rating operations in a cyber–physical power system network," *Sustain. Energy, Grids Netw.*, vol. 35, 2023, Art. no. 101140.

[10] B. Jimada-Ojuolape and J. Teh, "Composite reliability impacts of synchrophasor-based DTR and SIPS cyber–physical systems," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3927–3938, Sep. 2022.

[11] B. Jimada-Ojuolape, J. Teh, and C.-M. Lai, "Securing the grid: A comprehensive analysis of cybersecurity challenges in PMU-based cyber-physical power networks," *Electric Power Syst. Res.*, vol. 233, Aug. 2024, Art. no. 110509.

[12] B. Jimada-Ojuolape and J. Teh, "Surveys on the reliability impacts of power system cyber–physical layers," *Sustain. Cities Soc.*, vol. 62, Nov. 2020, Art. no. 102384.

[13] D. P. Oyinloye, J. S. Teh, N. Jamil, and J. Teh, "SIM-P—A simplified consensus protocol simulator: Applications to proof of reputation-X and proof of contribution," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 5083–5094, Mar. 2023.

[14] *IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected With Electric Power Systems*, IEEE Standard 1547.3-2023 (Revision of IEEE Standard 1547.3-2007), Dec. 2023.
[15] J. Johnson, "Roadmap for photovoltaic cyber security," U.S. Department of Energy, Tech. Rep., SAND2017-13262, Dec. 2017.
[16] 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, 2020.
[17] J. Ye et al., "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.
[18] B. Ahn et al., "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Trans. Power Electron.*, vol. 39, no. 4, pp. 4657–4673, Apr. 2024.
[19] W. G. Schwartz, A. Corbitt, A. Broomfield, C. Farnell, and H. A. Mantooth, "Integration and field testing of a multilevel cybersecurity solution for photovoltaic systems," in. *Proc. IEEE Des. Methodol. Conf.*, Grenoble, France, 2024, pp. 1–7.
[20] 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 physically unclonable function (PUF)-Embedded security module," in *Proc. 6th IEEE Workshop Electron. Grid*, 2021, pp. 1–4.
[21] B. Ahn, K. Nakka, N. R. Handke, T. J. Reyna, and T. Kim, "Field demonstration of blockchain-based security for a solar farm," in *Proc. 2024 IEEE Energy Convers. Congr. Expo.*, 2024, pp. 1753–1759.
[22] B. Ahn, A. Jenkins, J. Massa, L. M. Silva, T. Kim, and S. Choi, "Disruption of commercial solar inverter system by tls proxy man-in-the-middle attack," in *Proc. IEEE 7th Int. Conf. Ind. Cyber-Phys. Syst.*, 2024, pp. 1–6.
[23] B. Ahn, A. M. Jenkins, T. Kim, J. Zeng, L. McLauchlan, and S.-W. Park, "Exploring ransomware attacks on smart inverters," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2023, pp. 1567–1573.
[24] MITRE, "ATT&CK for ICS," Accessed: Jul. 11, 2025. [Online]. Available: https://attack.mitre.org/matrices/ics/
[25] Q. Zhou, "Directed acyclic graphs," UCLA Dept. of Statistics, Accessed: Jul. 11, 2025. [Online]. Available: http://www.stat.ucla.edu/~zhou/courses/Stats212_DAG.pdf
[26] CVSS, Accessed: Jul. 11, 2025. [Online]. Available: https://www.first.org/cvss/
[27] SMA Sunny Boy, Accessed: Jul. 11, 2025. [Online]. Available: https://files.sma.de/downloads/SBxx-US-1XP-41-BA-en-11.pdf
[28] Enphase Envoy-S, Accessed: Jul. 11, 2025. [Online]. Available: https://enphase.com/download/envoy-s-installation-and-operation-manual
[29] D. Arnaldy and T. S. Hati, "Performance analysis of reverse proxy and web application firewall with telegram bot as attack notification on web server," in *Proc. 3rd Int. Conf. Comput. Inform. Eng.*, Yogyakarta, Indonesia, 2020, pp. 455–459.
[30] S. R. B. Alvee, B. Ahn, S. Ahmad, K.-T. Kim, T. Kim, and J. Zeng, "Device-centric firmware malware detection for smart inverters using deep transfer learning," in *Proc. 2022 IEEE Des. Methodol. Conf.*, 2022, pp. 1–5.
[31] Q. Li, J. Zhang, J. Ye, and W. Song, "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," in *Proc. 2022 IEEE Appl. Power Electron. Conf. Expo.*, Houston, TX, USA, 2022, pp. 1926–1930.
[32] "Bootkit smaple for firmware attacks," (n.d.). [Online]. Available: https://github.com/hardenedvault/bootkit-samples
[33] B. Ahn, "Open-source code for a BC reference code," (n.d.). [Online]. Available: https://github.com/beauahn/BCforPV

BoHyun Ahn (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Minnesota State University-Mankato, Mankato, MN, USA, in 2016 and 2018, respectively, and the Ph.D. degree in engineering (electrical engineering Specialization) from Texas A&M University-Kingsville, Kingsville, TX, USA, in 2024. He was with the National Renewable Energy Laboratories, Golden, CO, USA, in 2023. He is currently a Postdoctoral Fellow with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO, USA. His research interests include cyber-secure smart inverters, malware security, ethical hacking, memory forensics, and blockchain-assisted security. He was the recipient of 1st place in 2022 IEEE Energy Conversion Conference and Expo student demo project software competition.

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, Lincoln, NE, USA, in 2012 and 2015, respectively. In 2009, He was with the New and Renewable Energy Research Group of Korea Electrotechnology Research Institute, Changwon. He was also with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA, in 2013. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO, USA. His research interests include cyber-physical power and energy systems including cyber-physical system security, power electronics and cyber-resilient power systems, quantum machine learning and optimization, and blockchain. He is an IEEE PELS Representative on IEEE Blockchain Technical Community Governing Board. He was the recipient of the 2018 Myron Zucker Student–Faculty Grant Award from IEEE Foundation, best paper award in 2017 IEEE International Conference on Electro Information Technology, and first prize award in 2013 IEEE Industry Application Society Graduate Student Thesis Contest.

Kalyan Nakka received the B. Tech degree in mechanical engineering from the Indian Institute of Technology Dhanbad, Dhanbad, India, in 2016, and the M.S. degree in computer science in 2023 from Texas A&M University-Kingsville, Kingsville, TX, USA, where he is currently working toward the Ph.D. degree in computer science. He was a Mid-Senior Level Professional with 5 years of software engineering experience, Infosys and Soroco, India. His research interests include the intersection of deep learning, adversarial ML, and security of AI systems domains.

Jinchun Choi received the B.E. and M.S. degrees in computer engineering from Inha University, Incheon, South Korea, in 2011 and 2014, respectively, and the Ph.D. degree in computer science from the University of Central Florida, Orlando, FL, USA, in 2020. From 2020 to 2022, he was a Postdoctoral Researcher with Texas A&M University-Kingsville, Kingsville, TX, USA. He is currently a Senior Researcher with Electronics and Telecommunications Research Institute, Daejeon, South Korea. His research interests include cyber security, network security, IoT security, and blockchain.

Seerin Ahmad (Member, IEEE) received the B.S. degree in electrical engineering from Aligarh Muslim University, Aligarh, India, in 2017, and the M.S. degree in electrical engineering from the Budapest University of Technology and Economics, Budapest, Hungary, in 2019, the Ph.D. degree in engineering (electrical engineering Specialization) from Texas A&M University–Kingsville, Kingsville, TX, USA. He is currently an Engineer with American Electric Power in the System Performance Analysis Department. His research interests include cyber-resilient power systems, inverter-based resources, power system stability, distributed energy resource management systems, power electronics, and cybersecurity.

Hee-Yong Kwon received the B.S., M.S., and Ph.D. degrees in computer engineering from Inha University, Incheon, South Korea, in 2015, 2017, and 2024, respectively. He is currently a Postdoctoral Fellow with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO, USA. His research interests include communication system security, information security, and post-quantum cryptographic algorithms.

Nathanial R. Handke is currently working toward the B.S. degree in electrical engineering with minors in mathematics and computer science, Texas A&M University-Kingsville, Kingsville, TX, USA. He was with Qualcomm, San Diego, CA, USA, in 2025. His research interests include GPU architecture, high-performance computing, quantum computing, and cybersecurity.

Trevor J. Reyna received the B.S. degree in electrical engineering from Texas A&M University-Kingsville, Kingsville, TX, USA, in 2024. He was an NSF Undergraduate Summer Intern with Cyber-Physical Power and Energy Systems Laboratory, Texas A&M University-Kingsville. His research interests include solar inverter hardware and control systems.