Field Demonstration of Blockchain-based Security for a Solar Farm

BoHyun Ahn
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
bohyun.ahn@students.tamuk.edu

Kalyan Nakka
Dept. of Computer Science and Engineering
Texas A&M University
College Station, TX 77843 USA
kalyan@tamu.edu

Nathanial R. Handke
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
nathanial.handke@students.tamuk.edu

Trevor J. Reyna
Dept. of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX 78363 USA
trevor.reyna@students.tamuk.edu

Taesic Kim*
Dept. of Electrical Engineering and Computer Science
University of Missouri-Columbia
Columbia, MO 65211 USA
tkx96@missouri.edu

2024 IEEE Energy Conversion Congress and Exposition (ECCE) | 979-8-3503-7606-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ECCE55643.2024.10860909

***Abstract*—This paper introduces a Blockchain (BC)-based security model for a solar farm, providing security functions such as firmware patching management, role-based access control, public key infrastructure, and man-in-the-middle attacks detection (MITM), malware file detection. In particular, this paper provides detailed field-testing methods at a solar fam to demonstrate the feasibility and effectiveness of cyber-attack detection methods. Practical cyberattacks targeting solar farms are designed and conducted. It is demonstrated that the proposed BC-based system proactively detects MITM attacks, firmware modification attack, and malware attack, while ensuring the continuous operation of the solar farm during attack events.**

Keywords—Blockchain, cybersecurity, malware detection, security module, smart inverter, security testbed, solar farm

I. Introduction

Solar capacity is projected to rise from the current 3% (80 GWac) of total U.S. electricity to 40% (1,000 GWac) by 2035 and further to 45% by 2050 (1,600 GWac) [1] to achieve national objectives related to decarbonization, power grid automation, and energy security improvement [2]. Solar inverters, crucial cyber-informed power-electronic devices, offer significant advantages within solar farms [3], including real-time remote access, critical data monitoring, parameter setting adjustments, and seamless implementation of over-the-air firmware updates [3] in a cyber-physical environment [4]. Despite these advantages, the extensive online information exchange among solar farm systems and diverse energy stakeholders—utilities, aggregators, vendors, operators, and owners—raises significant cybersecurity concerns [5]. These concerns include potential damage to valuable assets, threats to human safety, and substantial disruptions to the operation of the distribution power grid [6].

For example, in 2019, a cyber threat actor executed a Denial of Service (DOS) attack, causing a temporary loss of visibility for renewable energy system operators overseeing 500 MWac of wind and solar sites [7]. In 2022, the Dutch Radiocommunications Agency assessed the potential cybersecurity risks posed by solar inverter products to the PV system and the electric power grid in the Netherlands [8]. By tampering with inverter firmware (i.e., firmware malware), an attacker successfully accessed the personal data of Dutch customers, created new customer profiles, and deleted existing user accounts. Additionally, the attacker managed to obtain electricity generation data from customers' solar panels using GPS coordinates. In 2023, although specific details regarding the impacts of hacking were not disclosed, it was found that sensitive data from over 130,000 PV energy monitoring systems were publicly exposed online, potentially enabling nefarious remote access (i.e., Backdoor) to PV products [9]. Moreover, a demonstration showcased a malicious manipulation of numerous solar inverters from various well-known manufacturers in Germany [10]. This manipulation exploited vulnerabilities in unsecured firmware updates within a cloud-connected PV system. Publicly disclosed cyberattacks on commercial solar inverters, such as practical attack models [3], firmware malware attack [8], [10], as well as compromises to the IT systems of solar farms [7], highlight the urgency protecting PV systems and their endpoint PV devices from emerging cyber threats. Furthermore, ensuring their security has become indispensable for the reliability of the electric power grid [11].

The current cybersecurity of PV systems relies on standard and its network-based security measures such as user authentication, firewall rules, and encryption of network communication using Transport Layer Security (TLS) protocol [12], [13]. Beyond these existing security methods, Blockchain (BC) technology can offer a more secure distributed and private system framework compared to current information and communication technology (ICT) applications by leveraging the latest in cryptography, public key infrastructure (PKI), consensus, and role-based access control mechanisms, as recommended by IEEE 1547.3-2023 [14]. To deploy BC technology within current PV systems, this study utilizes the Hyperledger Fabric BC platform [15]. This platform, an open-source, enterprise-level, permissioned distributed ledger technology (DLT), is designed for implementation in settings with select, trusted participants, forming a private BC network. Among BC platforms, Hyperledger Fabric features a highly modular and configurable architecture, promoting innovation, adaptability, and optimization across a wide range of industry use cases.

This work was supported in part by the National Science Foundation (NSF) under award No. CNS-2219733 and the Department of Energy (DOE) under award No. DE-EE0009026.

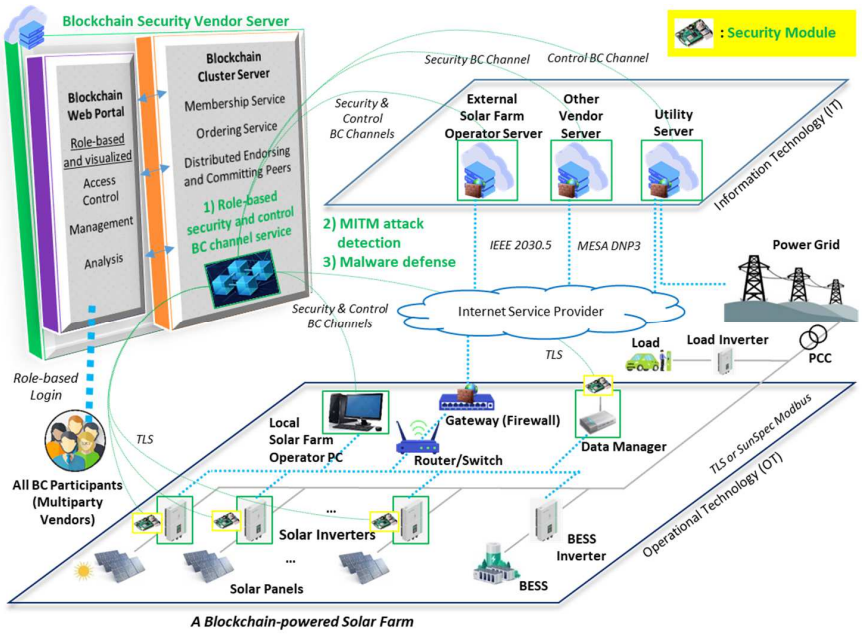


Fig. 1. A Blockchain-based security model applied to a solar farm.

To achieve a permissioned and flexible DLT, Hyperledger Fabric incorporates a multichannel function. This feature allows all multiparty participants to share the same data within a shared channel, or alternatively, permits partial participants to share data in a specific channel based on their permissioned and assigned roles. The studies [16] have applied the multichannel concept of Hyperledger Fabric to various systems: internet-accessible vehicles and battery management systems. Additionally, the previous study [17] introduced the initial version of a solar farm-tailored BC security testbed and defense methods and employed a separate single channel for the security aspects of received control commands and firmware for a solar inverter within a PV system, aimed at detecting malicious events. However, this earlier version was limited to a lab-scale environment, requiring extra hardware, software resources, as well as additional time for setup and experimentation.

Field testing related to cybersecurity in solar farms has seldom been publicly disclosed. Hence, the primary contribution of this paper lies in its real and practical demonstration of a BC-based security system within a commercial solar farm. This system effectively defends against diverse cyberattacks and ensures uninterrupted operation of solar inverters during such events, thereby enhancing the security of grid-connected solar farms. Consequently, this paper can establish a foundational reference for cybersecurity in the energy sector, emphasizing the critical role of security-by-design principles in advancing national energy security goals.

II. The Concept of Blockchain-based Security for a Solar Farm

A. Blockchain-powered Solar Farm

Fig. 1 shows a conceptual BC-based solar farm. The integration of the BC technology can enhance the security of the existing solar farm by safeguarding endpoint PV devices {such as solar inverters and the site PV data manager (which manages multiple inverters)} and local/external solar farm managing servers/PCs. They are all BC client nodes (BC participants). An authorized BC security vendor server can establish a BC cluster server responsible for securely managing participants in both private membership service and distributed-and-integrated data information (BC ledger) manners between all participants. This cluster server also supports either a security BC channel, a command BC channel, or both, depending on the assigned participant role. Within this security vendor server, a BC Web Portal program is also integrated, offering role-based and visualized access control, management, and real-time analysis in interaction with the cluster system. Therefore, all solar farm BC participants can directly and easily access this BC Web Portal for intuitive and effective solar farm management.

B. Private Blockchain Technology

BC technology functions as a decentralized and tamper-proof database mechanism that facilitates transparent information sharing across a network. Its structure comprises a chain of interconnected blocks that store data. Because these blocks cannot be altered or deleted without network consensus, data remains consistently organized chronologically. This characteristic makes BC technology ideal for creating immutable ledgers that track historical data records, such as transactions. By decentralizing and securing data storage, the BC technology mitigates the vulnerabilities associated with centralized databases.

Hyperledger Fabric, a permissioned BC framework tailored for private and consortium networks, addresses the limitations of permissionless and public frameworks like Bitcoin and Ethereum. It operates on the Practical Byzantine Fault Tolerance (PBFT) consensus protocol, which minimizes computational demands compared to Proof-of-

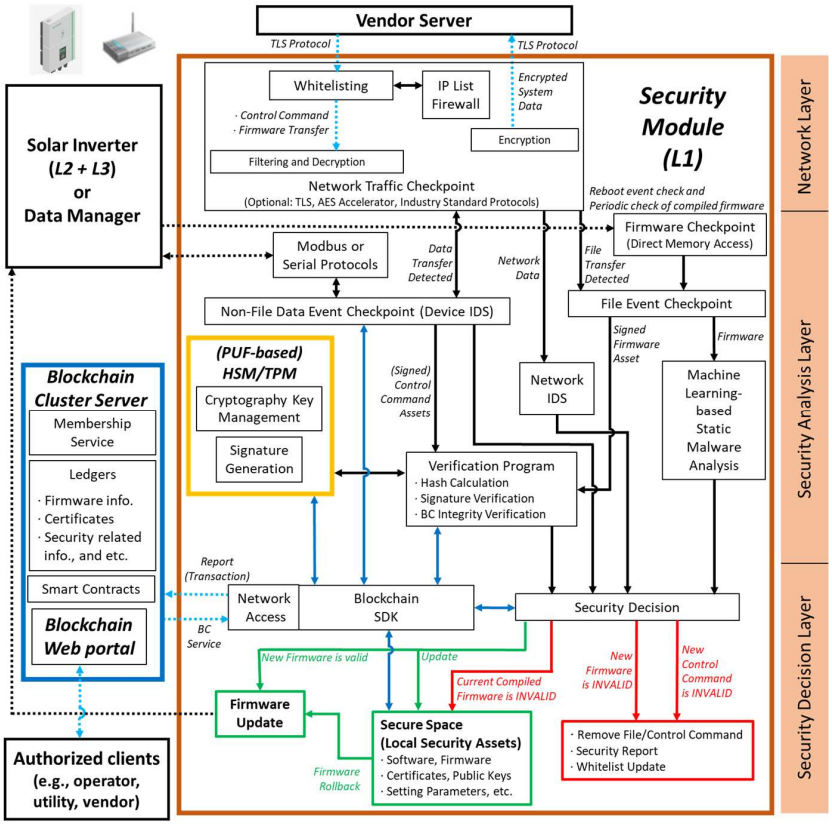


Fig. 2. A security module design.

Work (PoW), thereby reducing latency and resource requirements. The workflow of Hyperledger Fabric involves client/peer nodes proposing new transactions, which are validated by endorsing peers executing smart contracts (chaincode). Approved transactions are then processed by ordering peers to create a block, which is subsequently stored in a distributed manner among committing peers using PBFT. This permissioned, private, and distributed nature of Hyperledger Fabric enhances network resilience against faults.

C. Security Module

To establish an interface the solar farm with the proposed BC technology, a security module has been developed and integrated into each endpoint PV device [17], such as solar inverters and the site PV data manager. With respect to solar inverters, the security module software can be embedded into the network layer (*L1*) of the solar inverter, as defined in [3]. Alternatively, the security module hardware can replace or be additionally appended ([17], [18]) to *L1* to provide protection for the controller layer (*L2*) and the power electronics hardware layer (*L3*) within the solar inverter. Therefore, the security module-integrated PV devices act as BC client nodes that can directly interface with the main BC cluster server. The security module not only functions as the client for the BC network interface but also incorporates specialized security features designed for PV systems [17], depicted in Fig. 2. This approach provides flexibility in both software and hardware requirements for the security module, enabling straightforward deployment across various models of PV systems.

III. Field Testing Implementation

A. Cyberattack Test Cases

Through a combination of literature search, input from industry partners, and recent attack incident reports, as well as vulnerability analysis, PV system vulnerabilities were identified [3]. Based on this analysis, potential attack vectors were also defined [3] and five test cases (TCs) focused on cyberattacks intended to disrupt the operation of the solar farm. 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 false data injection attack (FDIA) and MITM attacks, while TC-4 and TC-5 are related to firmware update-related attacks involving malware or maliciously tampered firmware provided by compromised vendors.

B. Control Command Attack Test

Fig. 3 shows an implementation workflow for TC-2 describing local MITM attack and its defense by BC. A maliciously established device (Kali Linux) positioned between the data manager device and the solar inverter within the solar farm intercepts a valid control command (635), then tampers with it to an invalid control command (0). However, this attack is proactively detected and defended by the solar inverter security module in *L1* (the network layer of the solar inverter) through a verification process. This is achieved by leveraging BC integrity checks with all BC participants.

TABLE I
TEST CASES FOR THE FIELD TESTING AND BLOCKCHAIN-BASED DEFENSE RESULTS

TC	Attack Type	Vulnerability	Attack Vector (Way of Attack)	Description (Penetration Testing)	Goal of Attack	Average Defense Time	Accuracy
TC-1	External Network FDIA by MITM	PKI Vulnerability in TLS	1) A stolen TLS certificate key or 2) A maliciously exploited TLS CA could create external MITM attacks to generate a FDIA	An unidentified MITM proxy server compromises external control commands between vendor server and data manager	Target solar inverters are off or disrupted by available control commands	**7 seconds**	**100%**
TC-2	Local Network FDIA by MITM	Insecure Local Network Protocol	An unauthorized device is physically connected to the router 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		**13 seconds**	**100%**
TC-3	Device FDIA	Insecure Field Device	Through a malicious firmware update, the data manager is compromised, which enables the opening of a backdoor port. As a consequence, 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		**11 seconds**	**100%**
TC-4	Malware Attack	Insecure Vendor's Codesigning System	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	**15 seconds**	**100%**
TC-5	OTA Firmware Update Attack	Insecure Vendor's Codesigning System	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	**18 seconds**	**100%**

C. Malware Attack Test

Fig. 4 illustrates the workflow for TC-4, detailing a malware attack and its defense using BC technology. The external vendor server had been compromised by an attacker. Despite accurately reporting new firmware information from the vendor server to the BC server, a deliberate malware transfer targets the solar inverter. However, through a combination of a device-centric machine learning (ML)-based malware classification method [19] and the use of BC technology in the data manager security module, effective defense against such device malware attacks is achieved. The data manager security module detects and blocks this malware attack, preventing further transmission to the solar inverter. All BC verification records are stored in the BC cluster server and accessible via the BC Web Portal.

IV. FIELD TESTING RESULTS

The developed BC-based security system was successfully deployed in the field, and the average defense time and accuracy for all TCs are listed in Table 1. The average defense time was determined by multiple testing attempts (alpha testing in a university lab, a power system center, and the solar farm field), measuring the time from the start of each TC to the appearance of its final defense result on the BC Web Portal.

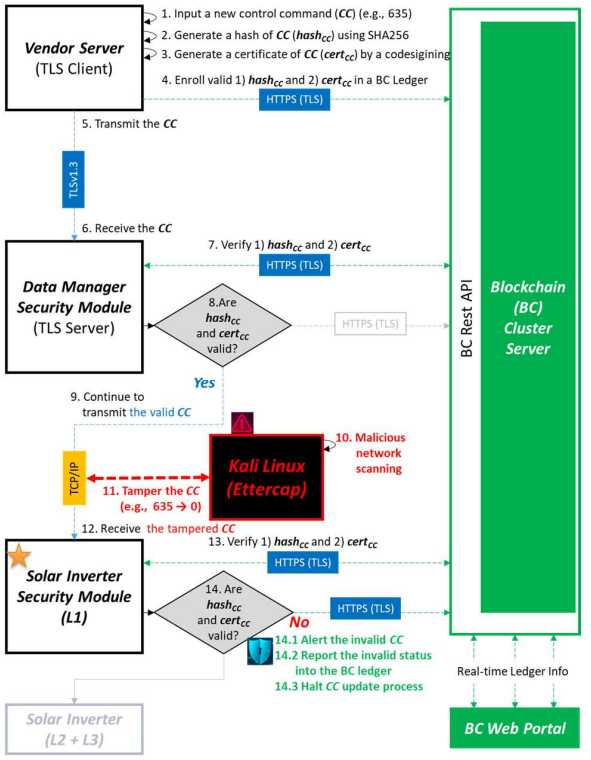


Fig. 3. Implementation workflow for TC-2 attack and its defense by Blockchain.

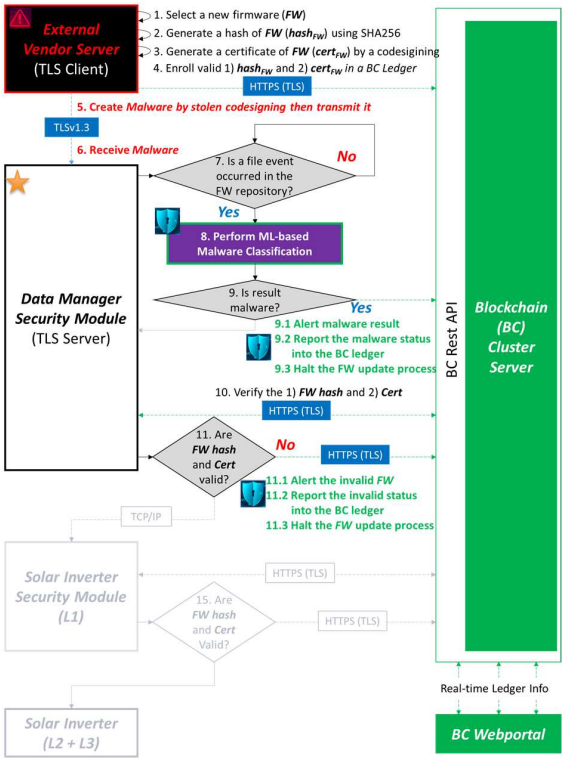


Fig. 4. Implementation flow diagram for TC-4 attack and its defense by Blockchain.

A. Experimental Setup

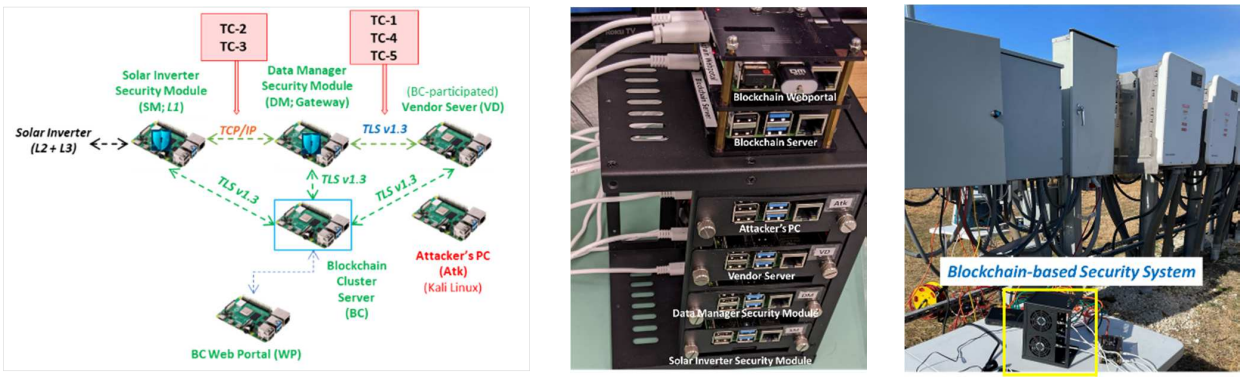
Fig. 5 illustrates the developed BC-based security system used for conducting defense demonstrations against the devised TC attacks in the solar farm. This system allows the operator to easily add and test cyberattacks for PV systems. Fig. 5(a) shows the hardware setup of the BC-based security system, highlighting each TC point for the field testing. Compared to the earlier BC-based security system introduced in [17], which required multiple PCs/laptops with different operating systems (OSs) mixed with IoT devices, the current system presented in this paper was developed using only 64-bit ARM processor-based, low-cost Raspberry Pi 4B devices. This was made possible by Hyperledger Fabric version 2.5's official support for ARM processors since early 2023. Additionally, the optimized and device-centric machine learning algorithm for malware detection, developed in [19], was successfully implemented on the Raspberry Pi 4B. This allowed the current version to include most of the intended security functions depicted in Fig. 2. Therefore, Fig. 5(b) illustrates the enhanced hardware system built with a Raspberry Pi 4B stack. This system was then seamlessly integrated into a commercial solar farm for demonstration purposes, as shown in Fig. 5(c).

B. Defense for Control Command Attack

Figs. 6 and 7 show the BC-based detection and defense results of the TC-2 attack in the field. Fig. 6 depicts a live screen view from the solar inverter security module, as seen from the perspective of the local solar farm operator via the BC software development kit (SDK). Following the scenario described in Fig. 3, the solar inverter security module (*L1*) received the control command (0) from the data manager. However, the integrity check of the command (0) failed due to its signature and hash were not valid when compared with the valid command (635) previously recorded in the ledger of the BC cluster server. Fig. 7 displays the intuitive BC Web Portal screen view from the perspectives of authorized role-based remote solar farm BC participants. All BC verification and defense records were displayed on the BC Web Portal. Since this control command was not valid, the solar inverter security module successfully blocked it to prevent further disruption to the solar inverter controller layer (*L2*) and the power electronic hardware layers (*L3*). The average duration for this defense test was 13 seconds with 100% accuracy. As a result, this ensured the continuous operation of solar inverters, thereby safeguarding the security of the grid-connected solar farm.

C. Defense for Malware Attack

Fig. 8 shows the results of malware detection (TC-4) by the data manager security module. Following the scenario described in Fig. 4, the data manager security module received a new firmware update from the compromised vendor server, which was automatically executated to a verification process through machine learning (ML). The verification result of the new firmware was classified it as malware. A detailed description of this device-centric ML algorithm can be found in [19]. Additionally, the data manager security module



(a) (b) (c)

Fig. 5. Blockchain-based security system for TCs: (a) system configuration; (b) system hardware, and (c) system deployment in a commercial solar farm.

Fig. 6. Defense result for TC-2: solar inverter security module screen via BC SDK.

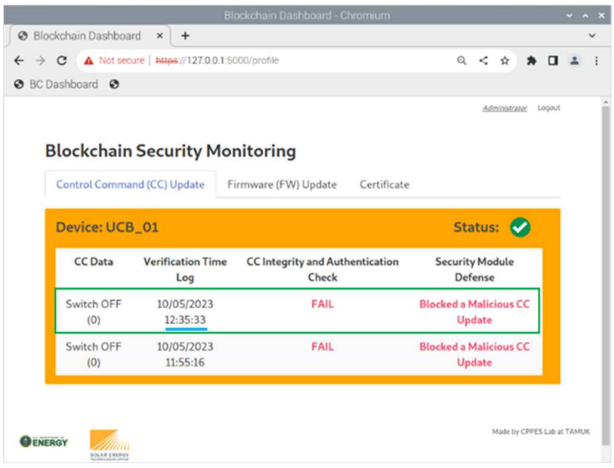


Fig. 7. Defense result for TC-2: Blockchain Web Portal screen.

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 cluster server. Fig. 9 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 security module, with integrity and authentication checks failing, and includes a timestamp for verification. 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 security module) with 100% accuracy. Consequently, the data manager security module effectively prevented the malware update to the solar inverter, ensuring its continuous operation.

V. Challenge and Discussion

The testing for TC-4 and TC-5 in the field encountered minor failures due to an activated commercial solar farm network security, which restricted any payload transfers within the field network. The system was programmed to automatically transfer files between the vendor server Raspberry Pi and the data manager security module Raspberry Pi using the *scp* protocol over SSH in a Python program for file transfer emulation purposes. However, even though this file transfer function failed, the BC-based security defense was achievable once the file was manually injected into the data manager security module for the devised verification process.

VI. Conclusion

To demonstrate the feasibility and effectiveness of Blockchain technology in mitigating potential cyber risks within solar farms, the field testing was conducted at a commercial solar farm using the developed BC-based security system against various devised cyberattacks targeting the solar farm. While the payload process was not automatically conducted due to the solar farm's network security, valuable insights were gained into the current security measures of solar farms and identified areas for improving the testing approach. However, this work still can 1) raise awareness among power engineering researchers about the impact of cyberattacks on solar energy systems and 2) secure PV

Fig. 8. Defense result for TC-4: data manager security module screen via BC SDK.

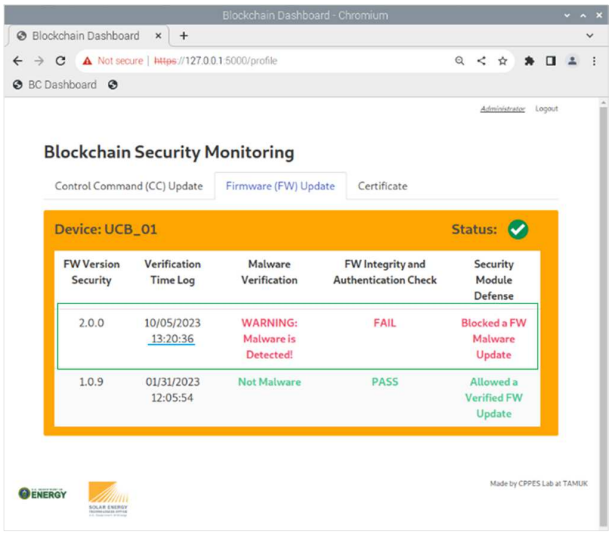


Fig. 9. Defense result for TC-4: Blockchain Web Portal screen.

systems against evolving energy cyberattacks involving malware.

Future work includes 1) enhancing the current BC-based security system to automatically transfer payloads in the solar farm with more realistic file transfer method and securely bypassing the network security for the ethical testing purpose and 2) developing advanced defense methods for PV systems against new attack vectors such as Generative AI-based attacks and post quantum cryptography (PQC) attacks.

REFERENCES

[1] The U.S. Department of Energy-SETO, "Solar futures study," Tech. Rep., GO-102021-5621, Sept. 2021.

[2] The U.S. Department of Energy (DOE), "Cybersecurity considerations for distributed energy resources on the U.S. electric grid," Oct. 2022.

[3] B. Ahn, T. Kim, S. Ahmad, S. Mazumder, J. Johnson, A. Mantooth, and C. Farnell, "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Trans. Power Electronics*, 2023, vol. 39, no. 4, pp. 4657–4673, April 2024.

[4] S. K. Mazumder et al., "A review of current research trends in powerelectronic innovations in cyber–physical systems," *IEEE J. Emerg. Sel.Topics Power Electron.*, vol. 9, no. 5, pp. 5146–5163, Oct. 2021.

[5] C. Lai *et al*., "Cyber security primer for DER vendors, aggregators, and grid operators," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND-2017-13113, Nov. 2017.

[6] J. Qi, A. Hahn, X. Lu, J. Wang, and C-C. Liu, "Cybersecurity for distributed energy resource and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, Dec. 2016.

[7] Catherine Stupp, "European wind-energy sector hit in wave of hacks," The Wall Street Journal. April 25, 2022. [Online]. Available: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000

[8] E. Bellini, "Dutch agency investigates cybersecurity of PV inverters after hack," pv magazine, September 6, 2022. [Online]. Available: https://www.pv-magazine.com/2022/09/06/dutch-agency-investigates-cybersecurity-of-pv-inverters-after-hack/

[9] B. Toulas, "Over 130,000 solar energy monitoring systems exposed online," BLEEPINGCOMPUTER, July 6, 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/

[10] Sebastien, "Decentralized energy production: green future or cybersecurity nightmare?," Dec. 30, 2023. [Online]. Available: https://media.ccc.de/v/37c3-11810-decentralized_energy_production_green_future_or_cybersecurity_nig-htmare/

[11] J. Ye, *et al*., "A review of cyber-physical security for photovoltaic system," in *IEEE Journal of Emerging and Selective Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, August 2022.

[12] J. Johnson, "Roadmap for photovoltaic cyber security," *Sandia Tech. Rep.*, SAND2017-13262, December 2017.

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

[14] "IEEE guide for cybersecurity of distributed energy resources interconnected with electric power systems," in IEEE Std 1547.3-2023 (Revision of IEEE Std 1547.3-2007), pp. 1–183, Dec. 2023.

[15] Hyperledger Fabric. [Online]. Available: https://www.hyperledger.org/use/fabric

[16] L. Gao, C. Wu, T. Yoshinaga, X. Chen and Y. Ji, "Multi-channel blockchain scheme for internet of vehicles," *IEEE Open Journal of the Computer Society*, vol. 2, no. 01, pp. 192-203, 2021.

[17] B. Ahn, G. Bere, S. Ahmad, J. Choi, and T. Kim, "Blockchain-enabled security module for transforming conventional inverters toward firmware security-enhanced smart inverters," in *Proc. 2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, Vancouver, BC, Canada, October 10–14, 2021, pp. 1307–1312.

[18] W. Hupp, A. Hasandka, R. S. de Carvalho, and D. Saleem, "ModuleOT: A hardware security module for operational technology," in *Proc. IEEE Texas Power Energy Conf.*, 2020, pp. 1–6.

[19] S. Alvee, B. Ahn, S. Ahmad, K. Kim, T. Kim, and J. Zeng, "Device-centric firmware malware detection for smart inverters using deep transfer learning," in *Proc. 2022 IEEE Design Methodologies Conferences*, Bath U.K., Sep. 1-2, 2022, pp. 1-5.