Blockchain-Based Communication and Data Security Framework for IoT-Enabled Micro Solar Inverters

Upamanyu Sinha, Abdullah A. Hadi, Tasnimun Faika, and Taesic Kim
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville
Kingsville, TX, USA
upamanyu.sinha@students.tamuk.edu; abdullah_al.hadi@students.tamuk.edu; tfaika@students.tamuk.edu;
taesic.kim@tamuk.edu

***Abstract*—It is expected that the conventional micro solar inverters can be revolutionized as a result of further investigation of the emerging Internet of Things (IoT) technologies and cloud computing services by providing continuous monitoring, data exchanging, and optimal operation in smart grid environments. However, there are imminent concerns and challenges regarding cybersecurity from cyber-attacks since the inverters through the IoT devices are always connected to networks such as Internet. The paper explores how blockchain technology could be used for potentially ensure communication and data security of the IoT-enabled micro solar inverters.**

Keywords—Blockchain, Hyperledger-Fabric, Internet of Things, IoT, micro solar inverter, smart contract

I. INTRODUCTION

Internet of Thing (IoT) is a concept that considers pervasive presence in the environment of a variety of things which can interact with each other through wireless and wired connections and cooperate with other things to create new applications/services and reach common goals [1].

The advent of IoT with cloud supports is expected to advance photovoltaic (PV) systems toward smart PV systems by fully utilizing IoT network, powerful cloud computing and resources including advanced analytics tools and visualization, resulting in providing significant value in cost reduction, extended scalability, greater visibility, and optimal control in smart grid environments. It has been noted that the IoT devices integrated in the PV inverters enable power monitoring [2] and health monitoring [3] services in cloud, and remotely controlling individual micro inverters via Internet. Moreover, the concept of IoT-enabled micro inverters support machine-to-machine communications leveraging decentralized optimal controls and peer to peer (P2P) electricity trading [4] in smart grid environments. However, there are critical concerns and eminent challenges regarding cybersecurity of IoT-enabled PV systems from cyber-attacks since the IoT-embedded micro solar inverters are always connected to Internet.

Cyber-attacks targeting the micro solar inverters will impose new security and safety risks, specifically, maliciously intending to damage or disable PV systems [5], [6]. Furthermore, the micro solar inverters with malware injected by hackers will be botnets that enable attacks other devices sharing networks in smart grid [7]. In addition, cloud services from the trusted party is still vulnerable to a single point of failure from cyber-attacks and challenge of longevity after vendors stop maintaining the cloud service [8]. With an awareness of these security concerns and challenges, investigation of the cybersecurity vulnerabilities (i.e., weaknesses) and guidance for mitigating cyber-attacks is imminently required to leverage the proliferation of the IoT-enabled PV systems.

Blockchain is a distributed database that maintains a continuously growing list of data records secured from tampering and revision [9]. Recently, blockchain technology incorporating blockchain ledgers and smart contracts (i.e., programing scripts) has been widely studied in many applications such as peer-to-peer (P2P) transaction, supply chain, energy trading [4], demand-side management [10], and IoT security and privacy [11]. However, the investigation of cybersecurity for IoT-enabled micro solar inverter in cyber-physical environments using blockchain technology has been not been studied to the best of authors' knowledge.

This paper aims to explore blockchain-based framework for exchanging data using blockchain ledgers and address potential opportunities and challenges for securing communication and data of the IoT-enabled micro inverters toward an improved cybersecurity in the PV systems. To validate the secure data sharing framework, an IoT-enabled micro solar inverter is built, where a developed smart contract is implemented in an IoT board integrated in a TI's micro inverter.

II. RELATED WORK

A. Communication and Data Vulnerability and Attacks of PV Systems

IoT devices or standard remote terminal units (RTUs) in the PV systems generally utilize lightweight network protocols which are not secure wired/wireless communication protocols due to the lack of encryption, access control, authorization and authentication. For example, message queuing telemetry transport (MQTT) is a simple publish-subscribe messaging protocol (i.e., IoT Pub/Sub) built on the top of TCP/IP protocol, which can be used in the PV systems or microgrids [12]. The MQTT protocol allows Publisher to broadcast messages on a topic to Subscribers who requested the topic messages via a Local Broker, as shown in Fig. 1. However, it is observed that the MQTT protocol still allows malicious subscribers to communicate with other devices [13]. Also, the entire IoT network will fail if the malicious subscriber can manage the broker since the broker can listen

978-1-7281-2925-9/19/$31.00 ©2019 IEEE

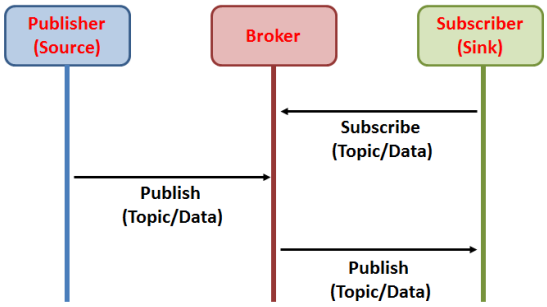

Fig. 1. Communication between publisher and subscriber in MQTT

to all messages send false messages. Other IoT communication protocols such as CoAP, XMPP, RPL and 6LoWPAN as well as standard RTU communication protocols such as Modbus and DNP3 are not secure by design as well. Therefore, unauthorized devices can access and manipulate the IoT network.

A man-in-the-middle attack (MITM) is a widely considered cyber-attack where the hacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other, as shown in Fig. 2. Potential examples of MITM include sniffer attack [14], and spoofing attack. A sniffer is an application or a device that can read, monitor, and capture network data exchanges and read network packets (e.g., Wireshark [15]) if the network is not properly encrypted. An attacker can create a fake router or website or unauthorized IoT devices. Such malicious devices or attackers can make spoofing attacks that actively manipulate exchanging data (i.e., data intrusion attacks), steal the private, and degrade network. Then, a hacker can make an attack point in the units of BMS by accessing any layers and installing a malware.

Furthermore, Denial-of-service (DOS) or distributed DOS attacks through the IoT network intend to shut down the PV systems accomplished by bonnets [16] that flood the targets (i.e., IoT devices or cloud) with huge network traffic or sending information that triggers a crash.

B. Blockchain Technology

Blockchain (e.g., Bitcoin [17] and Ethereum [18]) is an emerging technology used for secured transactions/database and network, which is a combination of trust mechanisms (e.g., distributed database and cryptography), a consensus algorithm, and smart contracts [18]). Blockchain is a distributed data structure consisting of timestamped blocks and links between blocks called "chain" and the blocks are inherently resistant to tampering and revision [9]. The general blockchain structure used in Bitcoin and Ethereum is shown in Fig. 3. A block consists of a block header and a body. The block header mainly includes block ID, a timestamp, a hash of the previous block (i.e., a cryptographic link creating a chain and tamper-proof), a random nonce (i.e., used for solving the proof of work (PoW)), and Merkle tree root (i.e., encoded transactions/data in the block in a single hash for efficient data verification; any data modification will change the hash value so that it is easy to check data integrity). The types of transaction will include records of the transfer of assets or data, broadcast messages, and smart contracts, which are encrypted by cryptographic digital signatures (e.g., users' private keys). Only participants who have the cryptographic keys can verify the data, time, and user of the transaction (i.e., data privacy). Therefore, such cryptographic methods will bring data integrity, privacy, and authentication.

Smart contracts are self-executing scripts that execute the terms of contracts triggered by designated events. If all the conditions of the contracts are satisfied, the blockchain network will execute the contract terms automatically and independently in a prescribed manner. Because a smart contract with a unique address is stored on the blockchain, users or nodes in the blockchain network can trigger the smart contract by addressing the transaction. Therefore, users have a capability of designing and implementing codes in the form of smart contracts for automated and efficient trading or workflows since smart contract provide an interface between the blockchain network and the physical world.

In view of the fact that the blockchain is hosted, updated, validated by individual peer nodes rather than by a single centralized authority, the blockchain improves the trust, security, and transparency of transactions/data due to inherent benefits such as immutability, auditability, data integrity and authentication, fault tolerance, and above all trust-free operation [9]. Moreover, the idea blockchain theory has brought about a potential solution to the IoT security problems [19].

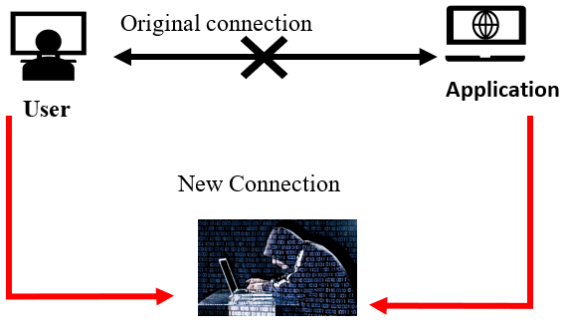

Fig. 2. MITM Attack

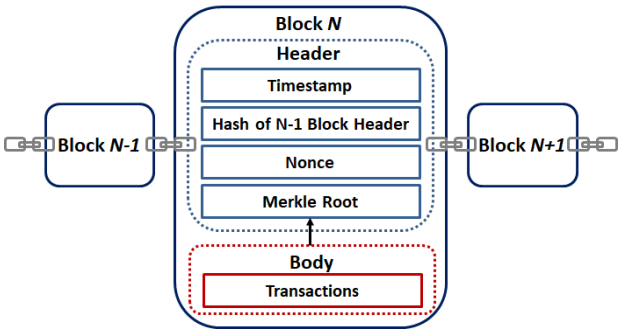

Fig. 3. General blockchain structure.

III. The Blockchain-Based Security Module Framework

A. Potential Communication and Data Security Improvement using Blockchain Technology

With blockchain technology in the PV systems, IoT-enabled micro inverters connected to the blockchain network will have own IDs and asymmetric keys. Therefore, communication in the PV system network will always be cryptographically proofed and signed by the sender, and thereby guaranteeing authentication and integrity of transmitted data [19]. Moreover, smart contract will provide users access control to restrict unauthorized access to the PV system network [20]. These features of blockchain authentication and access control can protect the MITM attacks in a private blockchain network. The effects of DOS attacks can be minimized by increasing transaction fees making DoS attacks more expensive and diversifying network connections using smart contracts. Therefore, illegal activity from network attacks (e.g., MITM attacks and DOS attacks) by using the blockchain technology.

With secured transmission data integrity, important data recorded on the distributed blockchain ledger and can be tracked securely, resulting increase in situational awareness. Data integrity in the data storage will be guaranteed by the distributed blockchain ledger using hash-based data encryption, identification, authentication, authorization, and verification of the ledgers by all blockchain network participants. Also, a single point of failure due the possibility of data manipulation by the cloud service provider will be mitigated using the distributed architecture with blockchain ledgers [20]. Therefore, any attempt to hack, steal or changing data in data storage will be detected and replaced with the original one.

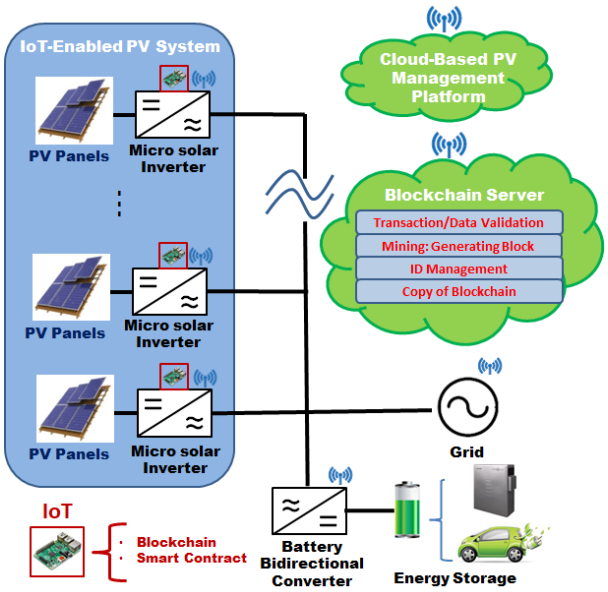

Fig. 4. A cyber-physical PV system consisting of an IoT-enabled PV system, a cloud-based PV management platform, and blockchain server in smart grid environments.

B. Communication and Data Vulnerability and Attacks of PV Systems

Fig. 4 shows the overall system architecture of a cyber-physical PV system consisting of an IoT-enable PV system, a cloud-based PV management platform, and a blockchain server in smart grid environments. The IoT-enabled PV system includes micro solar inverters integrating IoT devices. The cloud-based PV management platform will provide cloud services such as cloud-based PV power management, optimal control, health monitoring and energy trading, which however is not discussed in this paper. The blockchain server consisting of miners, peers, and validation nodes provides blockchain services such as transaction/data validation, mining, ID management, and blockchain ledgers.

In this paper, we propose the use of the IBM's Hyperledger-Fabric [22] that will be more applicable to the IoT applications than other blockchain platforms (e.g., Ethereum, and IoTA [23]) since the Hyperledger-Fabric provides private and permissioned blockchain, requires less energy and computational requirements in consensus protocols, and does not require transaction fees/coins. Based on the Hyperledger-Fabric, a smart contract (i.e., chain code) is designed for the micro inverters to: 1) broadcast messages/commands and sharing data through the blockchain ledgers; 2) exchange data which is not required to store in the blockchain ledgers through an encrypted private IoT network in the PV systems; and 3) store and read the shared BC ledgers. Therefore, the proposed blockchain-based framework can improve the communication and data security of the IoT-enabled micro inverters.

IV. Implemenation and Validation

Fig. 5 illustrates the experimental setup consisting of an IoT-enabled micro solar inverter, a PV simulator (i.e., DC power supply), a resistive load, an IoT device for an energy management system (EMS), and a blockchain sever built in a IBMS's virtual cloud server. The IoT device (i.e., LattePanda) is directly connected to a Piccolo-B (F28035) control card in the solar inverter and collects necessary information (e.g., voltage and current of the PV panel). Hyperledger-Fabric platform is implemented into the two IoT devices (i.e., clients) and the server acting as peer nodes and miner nodes in the BC

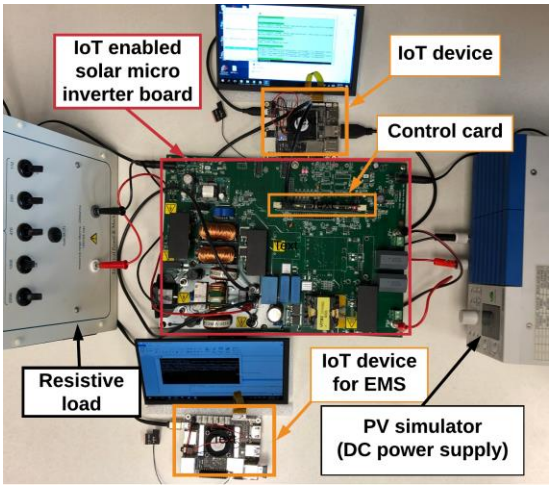

Fig. 5. Experimental setup.

network, respectively. Chain codes are written and implemented into the nodes.

Blockchain-based communication and data storage is executed as follows. First, the IoT-enabled micro inverter sends data to the blockchain server using encrypted Rest API. The data is then sent to the endorsement peers to validate the data with the chaincode. After validation, the data is sent to an orderer peer that sequences the data into a block. The block is sent to peer nodes and the cloud-based PV management platform. Finally, the data will be validated and connected to the peer's blockchain ledgers.

We validate a case of broadcasting PV data from the IoT-enabled micro inverter to the EMS through the BC ledger. Fig. 6 shows the PV voltages and currents in Data-1 and Data-2 recorded in the blockchain ledger stored in the EMS node. Therefore, the EMS can know the status of the PV system by reading data in the blockchain ledger. It is observed that it takes about 3 seconds until the EMS can see the PV data after the IoT-enabled micro inverter sent the data. This latency time will be further shorter if the blockchain server is locally installed, which gives a new opportunities and challenges of the adoption of the BC-based communication and data storage in the PV systems.

Furthermore, Fig. 7 shows the blockchain records of the RMS power supplied to the load from the solar micro inverter, which can be potentially used for transaction records.

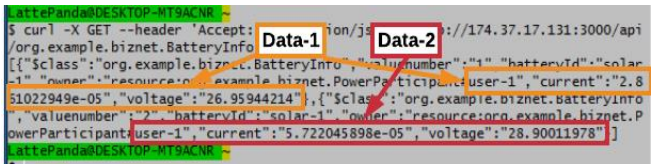

Fig. 6. Screen shot of PV data in the blockchain ledger.

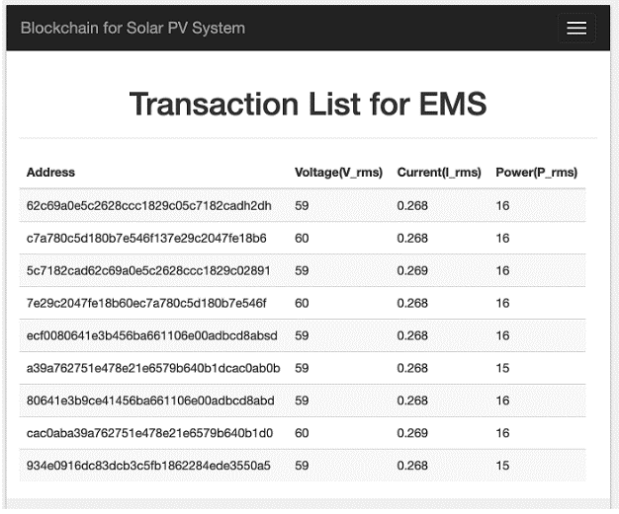

Fig. 7. Web-based user interface for energy transaction with Hyperledger Fabric.

V. Conclusions

This paper has introduced the BC-based communication and data security framework for the IoT-enabled micro solar inverters. It has been noted that the blockchain is promising to improve security of communication and data in the IoT-enabled PV systems. However, several challenges the currently available blockchain platforms: 1) the blockchain ledger grows in size, low communication complexity and high scalability, latency for real-time data exchanging, and the private keys with limited randomness. Future works include investigation of the cyber-physical security vulnerabilities and guidance for mitigating cyber-attacks through the combination of blockchain technology and artificial intelligence, proofing security strength of blockchain, and developing a new blockchain model to leverage the proliferation of the security-enhanced IoT-enabled PV systems in smart grid environments.

References

[1] O. Vermesan and P. Friess, Internet of Things-From Research and Innovation to Market Deployment, River Publishers, 2014.

[2] N. M. Kumar, K. Alturi, and S. Palaparthi, "Internet of Things (IoT) in photovoltaic systems," in *Proc. 2018 National Power Engineering Conference*, Madurai, India, Mar. 9-10, 2018, pp.1-4.

[3] M. N. Akram and S. Lotfifard, "Modeling and health monitoring of DC side of photovoltaic array," *IEEE Trans. Sustainable Energy*, vol. 6, no. 4, pp. 1245-1253, Oct. 2015.

[4] Microgrid Media, "It's like the early days of the internet, Blockchain-based microgrid tests P2P energy trading in Brooklyn," Mar. 2016.

[5] A. Teymouri, A. Mehrizi-Sani and C. Liu, "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, 2018, pp. 2872-2877.

[6] M. Chlela, D. Mascarella, G. Joos and M. Kassouf, "Cyber-resilient control of inverter based microgrids," *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Washington, DC, 2016, pp. 841-845.

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

[8] W. Hartzog and E. Selinger, "The internet of heirlooms and disposable things," *North Carolina JOTL*, vol. 17, no. 4, pp. 581–598, May 2015.

[9] N. Prusty, Building Blockchain projects, Packt Publishing, Feb. 2017.

[10] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proc. Conference on Control Technology and Application*, Mauna Lani, HI, , USA, Aug. 27-30, 2017. pp.1-8.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of things," *IEEE ACESS*, vol. 4, pp. 2292-2303, 2016.

[12] A. Adhikaree, H. Mankani, J. Kim, W. Qiao, and T. Kim, "IoT-enabled multiagent system for residential DC microgrids," in *Proc. 2017 IEEE International Conference on Electro Information Technology*, Lincoln, NE, May 14-17, 2017, pp. 100-104.

[13] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *Proc. 2018 IEEE Transportation Electrification Conference and Expo (ITEC)*, Long Beach, CA, 2018, pp. 934-938

[14] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," *IEEE Potentials*, vol. 21, no.5, pp.17-19, Dec. 2002-Jan. 2003.

[15] B. Wireshark, [Online] Available: https://www.wireshark.org/.

[16] C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress," DTIC Document, 2008.

[17] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[18] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum Project, Tech. Rep., 2014.

[19] M. A. Khan and K. Salah, "IoT security: review, blockchain solution, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and private: the study of a smart home," in *Proc. 2017 IEEE International Conf. Pervasive Computing and Communications Workshops*, Kona, HI, Mar. 13-17, 2017, pp. 618-623.

[21] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Network and Computer Applications*, vol. 125, pp. 251-279, 2019.

[22] Hyberledger-Fabric, [Online] Available, https://www.ibm.com/blockchain/hyperledger.html.

[23] IoTA, [Online] Available, https://www.iota.org/.