A Blockchain-Based Internet of Things (IoT) Network For Security-Enhanced Wireless Battery Management Systems

Tasnimun Faika, Taesic Kim, Justin Ochoa, Maleq Khan, Sung-won Park, and Chung S. Leung
Department of Electrical Engineering and Computer Science
Texas A&M University—Kingsville
Kingsville, TX 78363-8202 USA
tfaika@students.tamuk.edu; taesic.kim@tamuk.edu; justin.ochoa@students.tamuk.edu; maleq.khan@tamuk.edu;
sungwon.park@tamuk.edu; chung.leung@tamuk.edu

***Abstract*—Wireless battery management systems (WBMSs) are recently proposed to solve critical wiring-harness issues in conventional BMSs. It is expected that the emerging Internet of Things (IoT) and cloud computing technologies are expected to advance the WBMSs by fully utilizing IoT wireless network, powerful computing and unlimited cloud support, resulting in providing significant value in cost reduction, extended scalability, and greater visibility in the lithium-ion battery energy storage systems. However, the WBMSs present a growing threat from cyber-attacks as the WBMSs are always connected on networks and a lack of cybersecurity perspective is still prevalent in BMS usage and design phase. This paper explores blockchain technology for ensuring the communication and data security of an IoT-enabled WBMS from malicious cyber-attacks. The concept of the proposed blockchain-based IoT network for WBMSs is validated by experimental studies.**

Keywords—dual — blockchain, Hyperledger-Fabric, internet of things, IoT, smart contract, wireless battery management system

I. Introduction

Rechargeable lithium-ion (Li-ion) batteries are the widely utilized power source and energy storage devices for numerous electronic and electrical system applications such as portable electronic devices and electric vehicles (EVs) due to their high energy and power density, long service life, low self-discharge, and no memory effect [1]. However, properly designed battery management systems (BMSs) are necessary not only for ensuring their safety, reliability, optimal performance, but also for considering reduction of cost, weight, size, and manufacturing complexity [2]. The challenges of BMS design will be more significant as the number of battery cells increases [3].

A conventional BMS architecture typically includes a master BMS (MBMS) and module management systems (MMSs) for a battery pack consisting of the multiple battery modules [4] and utilizes wired communication systems (e.g., CAN, I^2C/SPI [5]) for module communication. The wired-communication in the BMS requires the installation of a large and complicated extra wiring, which causes the critical wire-harness issues [6]. Therefore, these will lead to increased cost, weight, and size, as well as decreased productivity and reliability.

Several wireless BMS architectures have been proposed to solve the wire harness issues in the conventional BMS using wired communication systems. Most of wireless BMSs (WBMSs) [6]-[8] are focused on wireless data transmission between sensors and a controller to minimizes/illuminates the wire-harness issues and enables the dispersed positions of the battery modules. In [8], an industry-first WBMS using a smart mesh embedded wireless network for EVs has been proposed by Linear Technology. Through the mesh network, each node is connected to neighbor nodes wirelessly with a fixed network topology and sends the data to a main node using neighbor nodes. However, such a centralized BMS network has critical drawbacks. Failure of the single leader node will lead to the failure of the entire system. Recently, a new distributed wireless Internet of Things (IoT) network-based WBMS has been proposed for an advanced, dispersed, and decentralized WBMS [9] , which utilizes IoT wireless network and cloud support toward a cyber-physical BMS [10], resulting in providing significant value in cost reduction, extended scalability, and greater visibility in the Li-ion battery energy storage systems. However, the WBMSs present a increasing threat from cyber-attacks since the wireless networks proposed for the WBMSs are not securely designed [11].

Cyber-attacks targeting the BMSs will impose new security and safety risks, specifically, maliciously intending to catch fire or explode batteries [11]. 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

This work was supported in part by the IEEE Foundation under IEEE IAS Myron Zucker Student-Faculty Grant Program 2018.

leverage the proliferation of the cyber-physical Li-ion battery energy storage systems using WBMSs. The research effort on cybersecurity for BMSs has recently been investigated. Summary of the cybersecurity research frameworks in BMSs may be found in [11], [12]. However, the actual approach to cybersecurity for BMSs in design phase has been less studied.

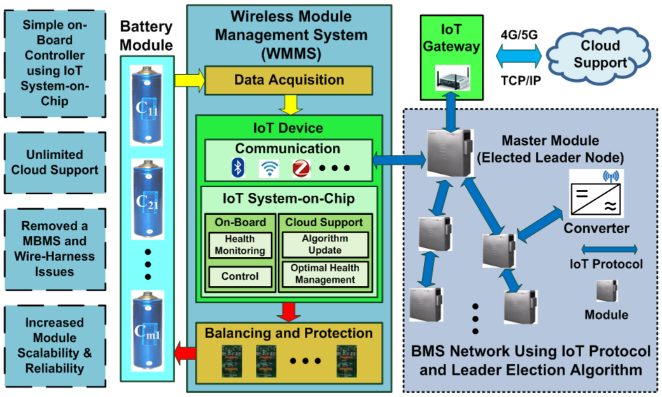
Blockchain is a distributed database that maintains a continuously growing list of data records secured from tampering and revision [13]. Recently, blockchain technology incorporating blockchain ledgers and smart contracts has been widely studied in many applications such as peer-to-peer (P2P) transaction, supply chain, energy trading [14], demand-side management [15], and IoT security and privacy [16]. However, the investigation of cybersecurity for BMSs in cyber-physical environments using blockchain technology has not been studied to the best of authors' knowledge.

The goal of this paper is to explore a blockchain-based IoT network for security enhanced WBMS. The proposed blockchain-IoT enabled BMS network can: 1) provide secure module-to-module communication and communication with external devices for decentralized BMS control through private channel with access control; and 2) securely store and exchange battery data with each module and share the data with a cloud server for battery health monitoring through the blockchain ledgers. The proposed IoT network is built using five Raspberry pi 3 IoT boards and a smart contract is implemented in each IoT board on Hyper-ledger Fabric blockchain platform to validate the. Experimental results validate the concept of the blockchain-based IoT network for the WBMSs.

II. Related Work

A. Overall Architecture of a WBMS

Fig. 1 shows the overall system architecture of a WBMS using a generic modular approach to BMS design that minimizes the communication wire-hardness issues and improves battery health monitoring and management through the IoT-cloud platform, resulting in a fully dispersed, decentralized, scalable, and adaptive cyber-physical BMS [9].



Simple on-Board Controller using IoT System-on-Chip
Unlimited Cloud Support
Removed a MBMS and Wire-Harness Issues
Increased Module Scalability & Reliability
Battery Module
C_{11}
C_{21}
C_{m1}
Wireless Module Management System (WMMS)
Data Acquisition
IoT Device
Communication
IoT System-on-Chip
On-Board
Health Monitoring
Control
Cloud Support
Algorithm Update
Optimal Health Management
Balancing and Protection
IoT Gateway
4G/5G
TCP/IP
Cloud Support
Master Module (Elected Leader Node)
Converter
IoT Protocol
Module
BMS Network Using IoT Protocol and Leader Election Algorithm

Fig. 1. The overall system architecture of the dispersed and decentralized wireless battery management system.

The IoT device is a key in the WMMS, which contains an IoT system-on-chip and a communication component (a short-range radio network, e.g., Wi-Fi, ZigBee, BLE) to communicate with other modules and external systems (e.g., a converter and energy management system) using MQTT protocol and an IoT Gateway connected to the cloud support server (e.g., battery condition monitoring and fault diagnosis cloud server [10]) via internet. Data acquisition and passive/active balancing are performed by a module monitoring IC that measures battery cell voltage, current, and temperature at given sampling time (e.g., Ts ≤ 1 second) and can balance the voltages of the cells when needed. Computationally efficient on-board battery health monitoring algorithms in a module estimates module SOC, capacity, and impedance and diagnose faulted cells [17]. The cloud support services include a secured on-board algorithm update based on the battery chemistry and an optimal health management based on the cloud-based comprehensive battery health monitoring results. Individual modules share duties of the master BMS and a leader module collects data from all other modules to know overall status of the battery pack. This approach can make the network operation much simpler.

B. Blockchain Technology

Blockchain Technology (e.g., Bitcoin [18], Ethereum [19], and Hyperledger-Fabric [20]) 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 [19]. 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. 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 the 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). 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. Therefore, such cryptographic methods will bring data confidentiality, integrity, and authentication.

Smart contracts are self-executing scripts that executes the terms of contracts. 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 the smart contracts with unique address are stored on the blockchains, users or nodes in the blockchain network can trigger a smart contract by addressing the transaction. Therefore, users can design and implement codes in the form of smart contracts for automated and efficient trading or workflows since smart contract provides interface between blockchain network and the physical world.

Since the blockchain is hosted, updated, validated by individual peer nodes rather than by a single centralized authority, the block chain 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 [13]. Moreover, the idea blockchain theory has brought about a potential solution to the IoT security problems [16].

III. Security Vulnerability of the IoT Network and Data Storage in WBMSs

A. IoT Network Vulnerability

WBMSs generally utilize simple and lightweight IoT protocols (e.g., MQTT [9]) which are less secure wireless communication protocols due to the weak of encryption, access control, authorization, authentication and identification mechanism [21]. For example, the MQTT protocol allows Publisher to broadcast messages on a topic to Subscribers who requested the topic messages via a Broker, as shown in Fig. 2. However, it is observed that the MQTT protocol still allows malicious subscribers to communicate with other devices. Also, the entire IoT network will fail if the malicious subscriber can manage the broker since the broker can listen to all messages send false messages.

In cryptography and computer security, a man-in-the-middle attack (MITM) is a widely considered network attack where the hacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other [11]. A potential example of MITM include sniffer attack [21] and spoofing. A sniffer is an application or a device that can read, monitor, and capture network data exchanges and read network packets (e.g., private data: login ID and password). An attacker can create a fake router or website or unauthorized IoT devices (or botnets). Such malicious devices can make spoofing attacks that: 1) repay routing information in the network layer protocol; 2) or make packet collision and dropping in the data link layer or 3) change exchanging data; 4) still the private data; and 5) use fake identities to degrade network (i.e., Sybil attacks [22]). Then, a hacker can make an attack point in the units of the BMS by accessing any layers and installing a malware.

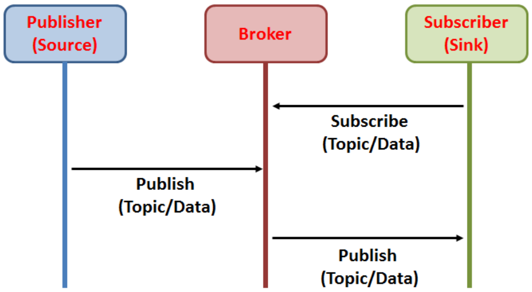


Fig. 2. Communication between publisher and subscriber in MQTT.

B. Data Integrity and Security Vulnerability

The Hackers can get an access to data storage in the BMSs and cloud if the devices/cloud are not properly locked. Once hackers steal privacy (e.g., login ID and password for data storage) or through malware injected in software after the end-to-end network attacks, it is possible that hackers can alter the data which is stored in data storage (e.g., voltage, current, temperature, and health related data such as SOC, SOH, and battery cell capacity). The altered data used in the on-board control algorithms and sent to the server will result in wrong monitoring outputs and control decisions. Therefore, data privacy, confidentiality and integrity will be easily violated.

Data privacy and integrity in the cloud supported IoT might be guaranteed by the cloud service providers (e.g., Google Cloud, Amazon Web Service, and Microsoft Azure). However, the IoT data and availability of cloud service is not always secured when login ID and password are stolen (i.e., a single point of failure). Moreover, only 82% of CSPs ensure communication data from IoT devices and only 10% of data is encrypted in the cloud data storage [23].

IV. Proposed Blockchain-Based IoT Network

In this paper, we propose the use of the IBM's Hyperledger-Fabric that will be more applicable to the IoT applications than other blockchain platforms (e.g., Ethereum and IoTA) since the Hyperledger-Fabric: 1) is private and permissioned blockchain providing access control (e.g., ID and key management); 2) requires less energy and computational requirements for consensus resulting in significantly less latency in creating a blockchain ledger compared to other platform; 3) does not require transaction fees/coins; and 4) can run smart contracts called "chaincode".

A. Blockchain for Communication and Data Security

Fig. 3 shows an architecture of blockchain network implemented in the IoT nodes in the WBMS and a blockchain

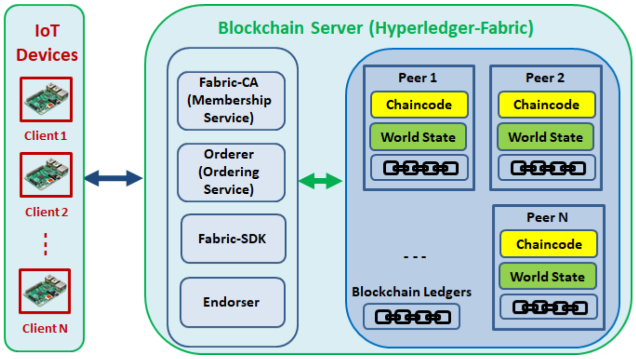


Fig. 3. Architecture of combining Blockchain and smart contract in the IoT-enabled solar micro inverters.

server. The blockchain server consists of miners and validation nodes and provides blockchain services such as transaction/data validation, mining, ID management, and copy of blockchain. The blockchain server can be implemented in a cloud server or a local server.

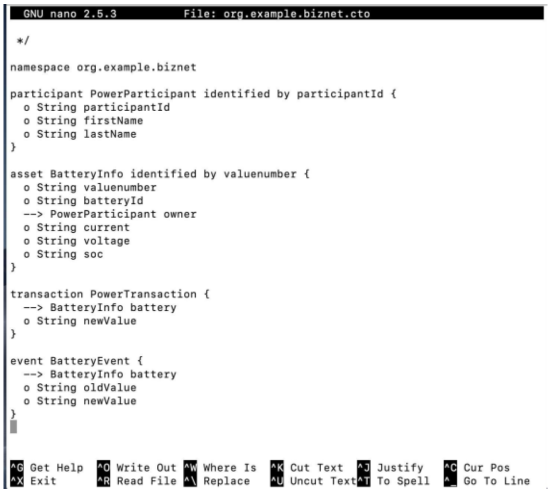
With blockchain technology, the IoT peer node can perform: 1) an interface that extracts data from the battery module (i.e., data aggregation) and controlling the module; 2) communication with other IoT nodes and cloud servers in the blockchain-based IoT network (e.g., private encrypted channels and blockchain ledgers); 3) store the shared blockchain ledgers; and 4) executing the smart contracts in the form of chaincodes. Therefore, it is expected that the IoT-enabled WBMS enables to: 1) share module status with each module to know overall status of the battery pack through blockchain ledgers, which illuminates the use of a reader election algorithm; 2) send battery health data to the cloud server for comprehensive health monitoring through the shared blockchain ledgers and 3) communication with other devices for decentralized BMS controls securely.

B. *Blockchain Implementation Using Hyperledger-Fabric*

As shown in Fig. 3, blockchain and smart contracts are implemented in the blockchain network which is constituent of IoT client nodes and a blockchain server called “Fabric” using the Hyperledger-Fabric platform. The IoT client node executes smart contract called “chaincode” in Hyperledger-Fabric. After enrolling the client via Fabric-CA (i.e., membership service) and a certificate is issued to the client. Then, the authorized client can communicate with a peer node in the blockchain server using fabric-sdk-node.

A block is made as follows. First, the IoT-enabled micro inverter sends data to the blockchain server using 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 peers.

Based on the Hyperledger-Fabric, chaincodes are designed for the battery module to: 1) send data/messages once it is available; 2) store and read the shared blockchain ledgers; and 3) exchange data which is not required to store in the BC ledgers through an encrypted private IoT network in the BMS; 4) defines the structure of the network. 5) keep synchronization among the nodes. An example code written for storing the battery data in the blockchain ledgers using Node.js, is shown in Fig. 4. Go language and java can also be used to write the chaincode.



```
  GNU nano 2.5.3          File: org.example.biznet.cto

 */

namespace org.example.biznet

participant PowerParticipant identified by participantId {
  o String participantId
  o String firstName
  o String lastName
}

asset BatteryInfo identified by valuenumber {
  o String valuenumber
  o String batteryId
  --> PowerParticipant owner
  o String current
  o String voltage
  o String soc
}

transaction PowerTransaction {
  --> BatteryInfo battery
  o String newValue
}

event BatteryEvent {
  --> BatteryInfo battery
  o String oldValue
  o String newValue
}


^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Fig. 4. An example chaincode.

V. Experimental Results

The proposed blockchain-based wireless IoT network for a WBMS consisting of five battery modules has been validated in a wireless IoT network testbed. Fig. 5 illustrates the wireless IoT network testbed built by using battery module emulators (BMEs), IBM Cloud (i.e., blockchain server), and an IoT Gateway (i.e., a router). The BMEs are designed by Raspberry pi 3 boards (i.e., IoT devices). The BME stores battery module data including cell voltage and current data (Ts = 1 second) generated by a battery cell simulation models [10] and Hyperledger-Fabric platform is implemented into the IoT devices and the blockchain server. Chain codes are written and implemented in both the server and the IOT devices to access and create the blockchain ledgers.

We validate a case of data exchange in the IoT nodes through the blockchain ledger. Fig. 6 shows the battery data including voltage, currents, SOC of cells recorded in the blockchain ledger, which is displayed on a web user interface in the Hyperledger-Fabric designed by a python flask web development tool. Moreover, the aggregated SOC values of the modules are illustrated in Fig. 7. Therefore, the any modules can know the current status of the battery system and the cloud support platform can execute a comprehensive battery health monitoring by reading data in the blockchain ledgers. Compared to the IoT network using unsecure MQTT protocol which takes about 1 and 3 seconds to aggregate data and elect a leader, respectively [9] in a similar test condition, the proposed network does not require a leader election

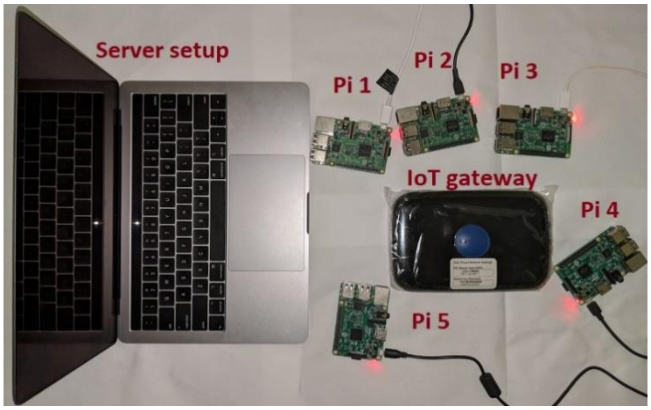
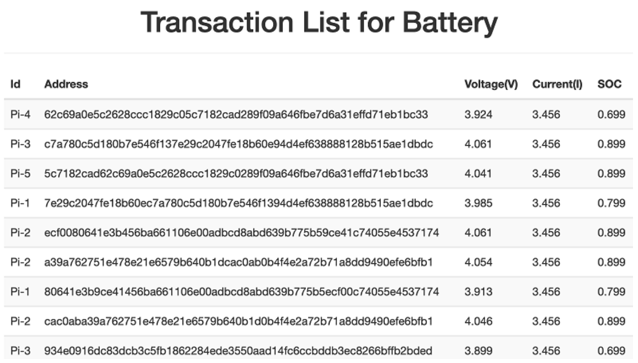


Fig. 5. Experimental setup.

algorithm and it takes about 3 seconds until a battery module can see the current status of the battery system after the IoT nodes sent the data. This latency will be still acceptable in the BMSs and further reduced if a local blockchain server is used instead of the cloud-based blockchain server. The results give new opportunities and challenges of the adoption of the blockchain-based communication and data storage in the battery systems.



Transaction List for Battery

Id	Address	Voltage(V)	Current(I)	SOC
Pi-4	62c69a0e5c2628ccc1829c05c7182cad289f09a646fbe7d6a31effd71eb1bc33	3.924	3.456	0.699
Pi-3	c7a780c5d180b7e546f137e29c2047fe18b60e94d4ef638888128b515ae1dbdc	4.061	3.456	0.899
Pi-5	5c7182cad62c69a0e5c2628ccc1829c0289f09a646fbe7d6a31effd71eb1bc33	4.041	3.456	0.899
Pi-1	7e29c2047fe18b60ec7a780c5d180b7e546f1394d4ef638888128b515ae1dbdc	3.985	3.456	0.799
Pi-2	ecf0080641e3b456ba661106e00adbcd8abd639b775b59ce41c74055e4537174	4.061	3.456	0.899
Pi-2	a39a762751e478e21e6579b640b1dcac0ab0b4f4e2a72b71a8dd9490efe6bfb1	4.054	3.456	0.899
Pi-1	80641e3b9ce41456ba661106e00adbcd8abd639b775b5ecf00c74055e4537174	3.913	3.456	0.799
Pi-2	cac0aba39a762751e478e21e6579b640b1d0b4f4e2a72b71a8dd9490efe6bfb1	4.046	3.456	0.899
Pi-3	934e0916dc83dcb3c5fb1862284ede3550aad14fc6ccbddb3ec8266bffb2bded	3.899	3.456	0.699

Fig. 6. Web-based user interface in Hyperledger Fabric.

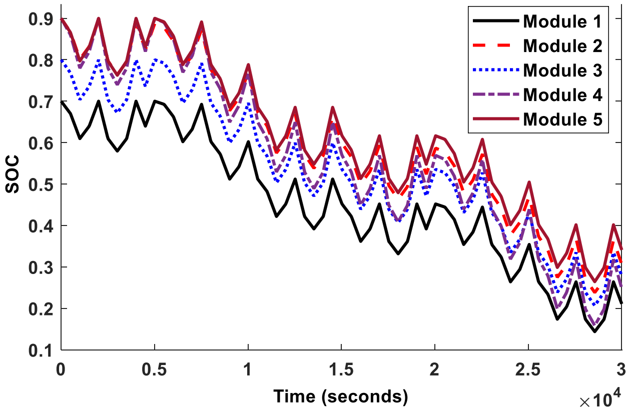


Fig. 7. The aggregated SOC values of the battery modules.

VI. Conclusions

This paper has introduced the architecture of a next generation WBMS in cyber-physical environments and its potential communication and data security threat from cyber-attacks. Moreover, this paper investigated blockchain-based IoT network for defense strategies in both communication and BMS data. The experimental results provide potential opportunity of enhancing cybersecurity of the WBMSs, which catalyzes the proliferation of the Li-ion battery systems in cyber-physical environments. Future works include comprehensive cybersecurity framework and experimental evaluations using the IoT-enabled BMS system and extending to other IoT-based systems.

References

[1] B. Scrosati and J. Garche "Lithium batteries: Status, prospects and future," J. *Power Sources*, vol. 195, no. 9, pp. 2419–2430, May 2010.

[2] J. Li, S. Zhou, and Y. Han, Advances in battery manufacturing, service, and management systems, IEEE Press Wiley, 2016.

[3] D. Andrea, Battery management systems for large Lithium-ion Battery Packs, Artech House, 2010.

[4] T. Kim, W. Qiao, and L. Qu, "A Multicell battery system design for electric and plug-in hybrid electric vehicles," in *Proc. 2012 IEEE International Electric Vehicle Conference*, Greenville, SC, USA, Mar. 4-8, 2012, pp. 1-7.

[5] P. Weicker, A systems approach to lithium-ion battery management, Artech House, 2014.

[6] M. Lee, J. Lee, I. Lee. J. Lee, and A. Chon, "Wireless battery management system," in *Proc. International Battery, Hybrid and Fuel Cell Electric Vehicle Symposium*, Barcelona, Spain, Nov. 2013, pp. 1-5.

[7] D. E. Alonso, Wireless data transmission for the battery management system of electric and hybrid vehicles, KIT Scientific Publishing, 2017.

[8] Electronic Publication: "Wireless battery management systems highlight industry's drive for higher reliability," Linear Technology Corporation, USA, 2017.

[9] T. Faika, T. Kim, and M. Khan, "An Internet of Things (IoT)-based network for dispersed, decentralized wireless battery management systems," in *Proc. 2018 IEEE Transportation Electrification Conference and Expo*, Long Beach, CA, June 13-15, 2018, pp. 1060-1064.

[10] T. Kim, A. Adhikaree, J. S. Vagdoda, D. Makwana, and Y. Lee, "Cloud-based battery condition monitoring and fault diagnosis platform for large-scale lithium-ion battery energy storage systems," *Energies*, vol. 11, no.1, pp. 1-15, Jan. 2018.

[11] 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*, Long Beach, CA, June 13-15, 2018, pp. 934-938.

[12] A. B. Lopez, K. Vatanparvar, A. P. D. Nath, S. Yang, S. Bhunia, M. A. A. Faruque, "A security perspective on battery systems of the Internet of Things," *J. Hardware and Systems Security*, vol. 1, no. 2, pp. 188-199, June 2017.

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

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

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

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

[17] T. Kim, A. Adhikaree, R. Pandey, D. Kang, M. Kim, C-Y Oh, and J. Baek, "An outlier mining-based real-time fault diagnosis for lithium-ion batteries using a low-priced microcontroller," in *Proc. 2018 Applied Power Electronics Conference and Exposition*, San Antonio, TX, Mar. 4-8, 2018, pp. 3365-3369.

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

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

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

[21] M. Abomhara and G. M. Koien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Security*, vol. 4, pp. 65-88, May 2015.

[22] L. Xiao, L. J. Green stein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Secur*. vol. 4, no. 3, pp. 492-503, 2009.

[23] AT&T Cybersecurity Insight, The CEO's guide to data security, Protect [Online] Available: https//www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf.