Critical Review on Intelligent Battery Management: Integration of Artificial Intelligence and Cybersecurity

Gaurav KUMAR and Suresh MIKKILI

***Abstract*—The adoption of lithium-ion batteries (LIBs) is rising in electric vehicles (EVs), data centers, and energy storage systems, due to their prolonged cycle life and enhanced safety performance. The battery packs incorporate a battery management system (BMS). BMS is vulnerable to cybersecurity risks because it depends on communication. We need to secure the reference values of battery voltage, current, and state of charge (SoC). If a hacker changes these values, the battery could be overcharged or undercharged. In this context, this paper discusses various communication protocols used in BMS, along with cell-balancing techniques, including active and passive ones. Furthermore, it enlightens the different SoC estimation techniques, such as artificial neural networks (ANN), model-based, data-driven, and statistical-based. These SoC methods are employed on an online dataset of a LIB. It indicates that the ANN has a minimum root mean square error (RMSE) of 0.1%. Moreover, blockchain is utilized to store the BMS data on a private blockchain network for anomaly detection. A hardware prototype is implemented to validate the anomaly data logging. The fabric network shows a maximum throughput rate of 312 for 500 transactions.**

***Index Terms*—Battery management system, blockchain technology, cybersecurity, cell balancing, state of charge estimation.**

I. Introduction

ELECTRIC vehicles (EVs) are a combination of hardware and software. Hardware includes microcontrollers, sensors, actuators, motors, high-power switches, diodes, an electronic control unit (ECU), and passive elements. The internal circuitry is connected using various communications modules such as a controller area network (CAN), bluetooth, ZigBee, FlexRay, and Modbus. Lithium-ion batteries (LIBs) are utilized in energy storage systems across battery-operated technologies, encompassing handheld electronic devices to EVs [1]. These batteries possess advantages, like higher power and energy density, extended lifespans, and minimal self-discharge rates. Nonetheless, LIBs have issues, especially safety hazards and performance decline caused by insufficient thermal stability and the aging phenomenon. The battery of EVs undergoes charging and discharging, causing the degradation of battery health and lifespan. Monitoring the state of charge (SoC) is essential to evaluate battery health. LIBs are configured in both series and parallel arrangements to form a high-capacity battery bank [2]. However, due to manufacturing variations, no two cells are identical even when they are produced in the same batch. The cells differ slightly in capacity, internal resistance, aging behavior, and leakage currents. A cell-balancing circuit is necessary to prevent the cells from overcharging or undercharging [3]–[7]. A battery management system (BMS) is necessary to equalize the voltages of series-connected cells and maintain uniform charge distribution across both series- and parallel-connected cells inside a battery pack. A BMS monitors battery parameters, such as SoC, protects the battery through charging and safety circuits, and communicates with ECU [8], [9]. The researchers are working on reducing the size and weight of the BMS [10]. In [11], a modular reconfigurable technique is proposed for energy storage systems. This technique supports series, parallel, and series-parallel connections with DC-DC converters. [12] introduced an ordered balancing architecture for modular DC reconfigurable battery packs (RBPs) designed to improve scalability and efficiency in extensive battery energy storage systems. A total of 48 V 3 Ah 18650 lithium-ion cells were employed in the experiment.

Several studies have been proposed by the researcher on wireless BMS (WBMS) [13], [14]. There are several methods in the literature, including the extended Kalman filter (EKF) [15], equivalent circuit models (ECMs), physics-based models [16], support vector machines (SVM) [17], artificial neural networks (ANN) [18], and deep neural networks (DNN) [19]–[21], to predict the SoC of batteries used in EVs.

Recent BMS are equipped with edge technology, including the internet of things (IoT), to communicate with the ECU [22]. The decision-making at the edge of BMS can be done using low-cost microcontrollers like NodeMCU, STM32, and Raspberry Pi microcontrollers. BMS faces issues with cyberattacks due to vulnerabilities in the communication layer. Cyberattacks can exploit the battery pack or alter battery data, including SoC values. Thus, it is important to protect BMS data from cyberattacks. There are four different types of attacks associated with BMS hardware and software components, including modification of data, interference in data, interception of data, and interruption of data [23].

Blockchain is a method for verifying and protecting sensitive information in a decentralized database. Blockchain refers

Manuscript received September 25, 2025; revised December 2, 2025 and January 14, 2026; accepted February 6, 2026. Date of publication June 30, 2026; date of current version March 11, 2026. This work was supported in part by Anusandhan National Research Foundation (ANRF) under the grant ANRF/PAIR/2025/000017/EPAIR. (*Corresponding author: Suresh Mikkili.*)

All authors are with Electrical and Electronics Engineering, National Institute of Technology Goa, Goa 403703, India (e-mail: gauravkumar@nitgoa.ac.in; mikkili.suresh@nitgoa.ac.in).

Digital Object Identifier 10.24295/CPSSTPEA.2026.00006

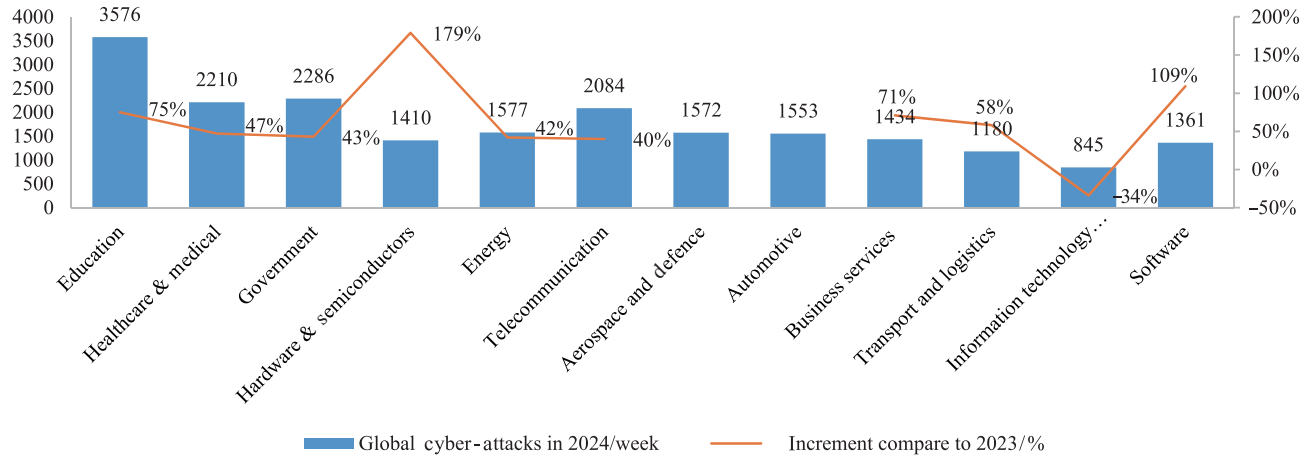


Fig. 1. Statistical data of global cyberattacks occurring in 2024 per week and percentage increment of attacks compared to the previous year

to a decentralized and distributed ledger technology (DLT) that accurately records transactions across numerous nodes, hence ensuring data integrity. The private blockchain is capable of digitally signing data from the sensors. It generates a digital signature for each piece of sensor data. It will help to enter only authorized EVs [24], [25]. Hyperledger Fabric can be used to integrate the client application using a smart contract and the MQTT IoT communication protocol.

This paper provides a critical review of BMS technologies and various cybersecurity threats, including hardware and software in BMS. Further, it discusses the modelling of a lithium battery using a third-order RC network. Moreover, various communications protocols are used in BMS, and SoC estimation techniques are discussed along with the integration of blockchain technology in BMS. SoC estimation is predicted using various methods. The proposed cybersecurity model is implemented using a single LIB.

The remaining paper is organized as follows: Section II focuses on cell balancing (CB) and cell modelling. Section III details the EV charging infrastructure, communication protocols, and cybersecurity threats. Section IV outlines the BMS and SoC estimation techniques. Section V reports the application of blockchain technology and its implementation. Finally, we conclude the paper in Section VI.

Recently, studies have focused on mitigating the cybersecurity issue [22], [26]. These perform the analysis on the realtime data gathered from the Netherlands' ElaadNL. Authors detect abnormal behaviour in the charging process by analyzing the parameters, where the charging data does not align with expected patterns, which could indicate problems and anomalies discussed in [27]. In [28], the authors developed a transfer learning model using weights from a DNN. This model improves detection accuracy by leveraging previously learned patterns from one dataset to another with 93% accuracy, 92.7% precision, 94.3% recall, and an F1 score of 93.1%. Hequan et al. [15] describe that EKF is combined with particle swarm optimization (PSO) and long short-term memory (LSTM) to enhance the prediction of the SoC of power batteries with 0.258% root mean square error (RMSE). [29] suggest artificial intelligence (AI) and blockchain applications in optimal charging schedules and secured decentralized EV charging. According to a report, global cyberattacks in various sectors are shown in Fig. 1 [30]. Table I provides a literature survey of various algorithms used for BMS technology in recent research, along with relevant remarks.

II. Modelling of Battery and CB Techniques

Various charging connectors are used worldwide, including CHAdeMO, CCS, Tesla Supercharger, type 1, type 2, GB/T, Chaoji, BHARAT AC, and BHARAT DC [34]–[37]. The charging connectors connect the eletric vehicle supply equipment (EVSE) with the EV for charging and communication. The open charge point protocol (OCPP) connects all EV chargers to the charging management server (CMS). However, connectors are used to charge the battery pack of EVs, but these communicate with EVs using CAN or a pulse width-based modulation technique. DoS attacks and man-in-the-middle attacks are shown in Fig. 2. A man-in-the-middle attack occurs between two networks. An attacker can interrupt the login and transaction-type security layers. The charging stations communicate with the CMS using OCPP. The central server provides the charger information to the payment gateway, charger owner, and EV users. The following subsections present the modelling of a LIB cell and an overview of CB techniques used in BMS to ensure uniform charge distribution.

Accurate battery modelling is essential for estimating SoC, predicting behaviour, and implementing protection and balancing strategies. The modelling for a single cell is done using the differential equations [38]. Fig. 3 shows the equivalent circuit of a single cell model. The model includes an open circuit voltage (OCV) source (V_{battery}), and internal resistance of the cell is (R_{int}) [5].

The expression for SoC can be written as $\frac{\mathrm{d}\,SoC}{\mathrm{d}t}=\frac{I(t)}{Q_{\mathrm{i}}}$

$$\dot{SoC}=\frac{I(t)}{Q_{\mathrm{i}}} \tag{1}$$

where $I(t)$ is the battery charging and discharging current, and

TABLE I
LITERATURE SURVEY OF DIFFERENT ALGORITHMS USED FOR BMS TECHNOLOGY IN RECENT RESEARCH WORK WITH REMARKS

Ref./Year	Paper content	Remark
[22]2024	Significance of EVs, challenges in EV adoption, role of BMS, cloud computing as a solution, and a comprehensive review of the analysis of recent research on cloud-based BMS frameworks and applications. Examination of existing industry solutions for BMS.	Emphasizes the potential of cloud computing used in BMS.
[15]2024	The paper introduces a novel SoC estimation method combining the EKF with PSO and LSTM models to enhance the accuracy.	The hybrid algorithm maintains RMSE within 0.258% and a maximum error below 1.55% across various conditions.
[29]2020	This article provides stakeholders and policymakers with insights into leveraging blockchain and AI for improving EV charging systems.	Blockchain networks could be used to address security and privacy issues in EV charging infrastructure. The three layers, networking, consensus, and transactions of the blockchain network, are discussed.
[31]2020	The function of V2G is explained in detail to stabilize the grid. The framework produces an optimal charging schedule for each electric vehicle, maximizing profits for owners while accommodating both their preferences and the demands of the grid.	An IoT- and edge-computing-based framework is developed for efficient V2G operation management using NodeMCU and Raspberry Pi hardware.
[32]2021	Traditional wired BMSs suffer from drawbacks such as extensive wiring complexity, limited scalability, increased system weight, higher deployment costs, and vulnerability to wiring failures.	The survey highlights the emerging trends, ongoing issues, and challenges in the field of WBMS, aiming to guide future research directions.
[24]2021	ECC is used for mutual authentication and key agreement between peers.	This study introduces a blockchain-enabled smart contract framework to manage demand response effectively during bidirectional energy exchange between electric vehicle batteries and the smart grid.
[25]2022	The article discusses the cybersecurity vulnerabilities that BMS may face due to potential cyberattacks and the need for robust defense strategies. Blockchain could provide a baseline reference for BMS developers to secure communication, data integrity, and operational security.	Blockchain transactions monitor and store BMS data.
[33]2024	This paper explains the application of LLM to provide security and privacy, as well as its inherent vulnerability.	LLMs can assist in analysing code and identifying vulnerabilities that could lead to security breaches.

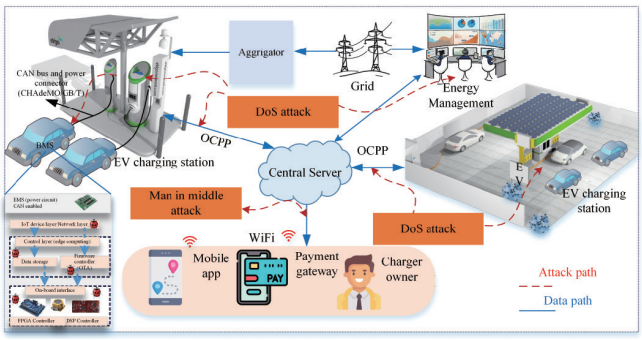


Fig. 2. Illustration of cyberattacks in the EV charging infrastructure.

Q_i is the capacity of the cell in ampere-seconds. The OCV of the battery ($V_{battery}$) is the function of SoC, and the battery current is calculated as given in (3).

$$\begin{cases} \dot{V}_1(t) = -\dfrac{1}{R_1C_1}V_1(t) + \dfrac{1}{C_1}I(t) \\ \dot{V}_2(t) = -\dfrac{1}{R_2C_2}V_2(t) + \dfrac{1}{C_2}I(t) \\ \dot{V}_3(t) = -\dfrac{1}{R_3C_3}V_3(t) + \dfrac{1}{C_3}I(t) \end{cases} \tag{2}$$

$$V_t(t) = V_{battery}(SoC) - I(t)\,R_{int} - V_1(t) - V_2(t) - V_3(t) \tag{3}$$

where R_1, C_1, R_2, C_2, R_3 and C_3 are the diffusion resistance and diffusion capacitance.

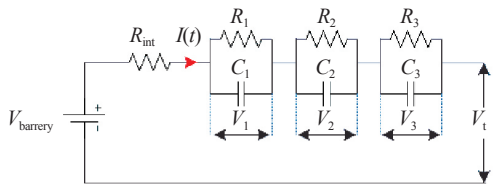


Fig. 3. Third-order RC model of a single cell.

LIB packs are made by connecting multiple cells in series and parallel to get the required voltage and current. The variations arising from manufacturing tolerances, aging, and operating conditions can cause individual cells in a series string to exhibit unequal voltages and SoC. In the lack of balancing, such imbalances may lead to overcharging or excessive discharging of certain cells, compromising safety and performance. CB circuits are therefore employed to regulate and equalize the charge levels across all cells within the battery pack. The classification of CB circuits, based on energy conversion techniques including active and passive balancing and control variables, is discussed in [5], [39].

A. Active Balancing (AB)

Transfer of charge is done between cells in a battery pack to equalize the voltage or SoC across all cells using capacitors, inductors, or transformers [40]. An H-bridge and DC-DC con-

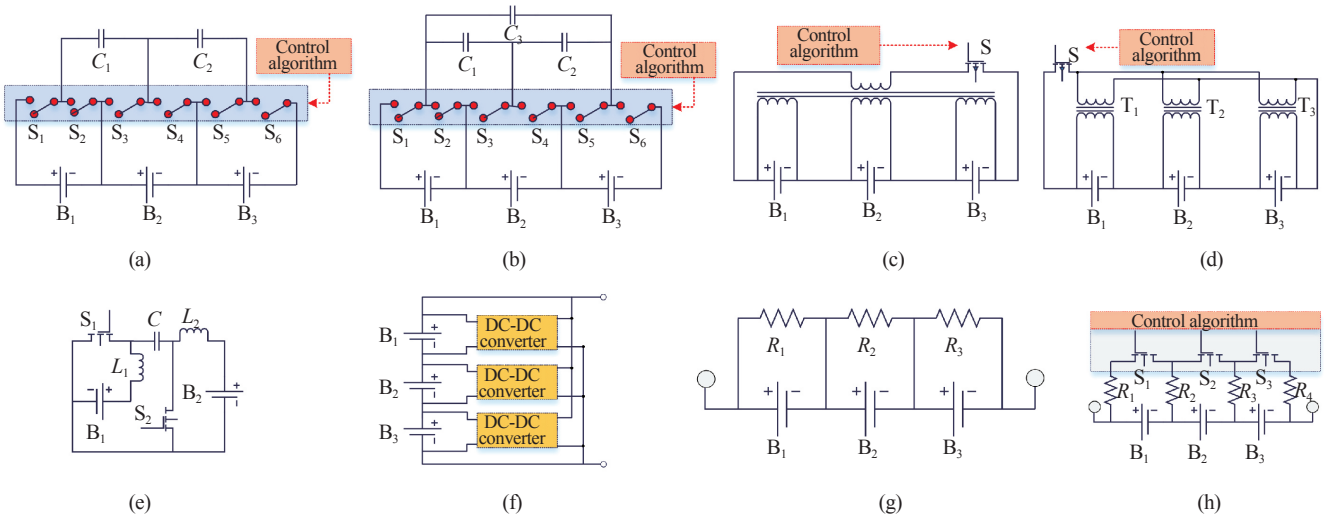


Fig. 4. Various CB techniques: (a) Capacitor-based AB, (b) two-layer capacitor-based AB, (c) multi-winding transformer-based AB, (d) single transformer-based AB, (e) Cuk converter-based AB, (f) single-converter-based AB, (g) fixed resistor-based passive CB, and (h) switched shunt resistor-based passive CB.

verter-based CB technique is proposed for series-connected cells. The minimum CB time is 400 s [41]. A flyback transformer-based active CB method with model predictive control and fuzzy logic control is discussed in [11]. The following AB techniques are given below:

1) Capacitor-Based AB

Capacitors are used to distribute the charge of the cell equally, as explained in [42]. These are charged through high voltage and discharged to lower voltage cells, as shown in Fig. 4(a). There are two topologies for capacitor-based CB circuits. These are single-layer switched capacitors and double-layer switched capacitors. A two-layer capacitor topology is used for transferring energy between cells. This configuration has the advantage over the single-switched capacitor method, as the second capacitor tier reduces the balancing time by more than half, as shown in Fig. 4(b). Dynamic voltage across capacitor $V_c(t)$ is given by (4).

$$V_c(t) = V_o + \frac{1}{C}\int_0^t I(t)\mathrm{d}t \tag{4}$$

where V_o is the voltage at $t = 0$ and I is the capacitor current.

2) Inductor-Based AB

The cells of the battery pack are connected with a single inductor or multiple inductors. A BMS circuit is used to switch the inductors by measuring the SoC of each cell. Charge flows from the high SoC to the low SoC cell.

This method has heat dissipation during the CB process. Switched capacitor and inductor topologies are given in [43]. The voltage across the inductor while the switch is closed is given in (5).

$$V_L(t) = I(t)R_L + L\frac{\mathrm{d}I(t)}{\mathrm{d}t} + I(t)R_{sw} \tag{5}$$

where R_{sw} is the voltage drop across the switch, V_L is the voltage drop across the inductor, and R_L is the inductor resistance.

3) Transformer-Based CB

The capacitor is replaced with a coil of a transformer with a switch. There are two different topologies with such transformer-based topologies. Multi-winding transformer topology and a single transformer are connected with each cell, as shown in Fig. 4(c) and (d), respectively. Two cells are balanced using the active transformer-based topology explained in [44].

4) DC-DC Converter-Based CB

A DC-DC converter is connected to each cell to maintain a constant voltage. The converter works in constant voltage mode. This topology is efficient compared to others because DC-DC converters have an efficiency of more than 95%. A non-inverting buck-boost converter is used for six series and one parallel-connected cell. An field-programmable gate array (FPGA)-based real-time simulator (OPAL-RT) is used for the validation of the proposed technique. For experiment validation, a 22 V, 2200 mAh battery pack is used; the efficiency during the experiment is 97.05% [6]. Fig. 4(e) shows the Cuk converter topology used for the charge balancing of two cells. Energy flows from one cell to another cell through L_1 and C components. Fig. 4(f) shows a single cell with a single converter to maintain its voltage corresponding to 100% SoC.

B. Passive CB

A basic BMS function is CB, which ensures uniform cell performance. This work [7] reviews recent advances in CB techniques for EVs, including traditional passive and AB methods as well as newer AI, machine learning, and ANN-based approaches. The study compares different methods using circuit models, equations, and case studies, highlighting their advantages and limitations. In the fixed resistor technique, the excess charge is dissipated through an external resistor to balance the charge of all the cells. This method is not suitable for the practical BMS because excess charge is converted to heat [45].

TABLE II
COMPARISON OF DIFFERENT CB METHODS

Category	Method	Research Gap	Efficiency	Cost	Complexity	Applications	Balancing speed
AB [6]2024	Non-inverting buck-boost converter	The topology has fewer components to reduce the loss and enhance the performance.	High (97.05%)	Medium	Medium	LIB pack	Fast (1328 s)
AB [11]2025	DC-DC converter	Four battery cells took 450 s for SoC balancing. The DSpace controller is used to implement the proposed algorithm.	–	Low	Low	Energy storage systems	Fast
AB [40]2025	State of power	Voltage/SoC-based methods do not optimize for power delivery or full cell usage.	High (16% increase)	Medium	High	–	–
AB [41]2024	Hybrid duty cycle DC converter	It controls each cell compared to other techniques.	80%	Medium	Medium	EV battery packs	400 s
AB [42]2014	Switched capacitor and inductor	Single-layer switched capacitors are used. A chain structure is proposed.	97.61%	Low	Low	Satellite and EVs	247 min
PB [7]2025	Fixed shunt resistor	Very slow	More than 90%	Low	Low	LIB pack	Slow
PB [7]2025	Switched shunt resistor	Slow	90%–95 %	Low	Low	LIB pack	Slow
PB [46]2018	Zener diode-based methods	Slow	High	Low	Very low	LIB pack	Slow
PB [47]2024	Passive CB, resistor-based	It is a slow technique	–	Low	Low	Battery packs of EVs	Slow balancing speed

1) Fixed Parallel Resistor Topology

The high-voltage cells will experience a higher balancing current flowing through their parallel resistances compared to low-voltage cells. The resistance across each cell is the same as shown in Fig. 4(g). Shunt resistance has a power dissipation issue. To overcome this resistance, a Zener diode is used.

The expression for energy dissipation is given by (6).

$$E(t) = V(t) \times I(t) \times T \tag{6}$$

where E is the energy dissipated in the resistor during CB, V is the voltage drop across the resistor, and T is the time required to dissipate the charge.

2) Parallel Zener Diode Topology

Zener diodes allow current to flow only when the voltage exceeds a specific threshold. To overcome the power dissipation issue, the shunt resistor is replaced with a Zener diode.

$$I_z = \frac{V_{cell} - V_Z}{R_Z} \tag{7}$$

where V_z is the Zener breakdown voltage and V_{cell} is the cell voltage when $V_z < V_{cell}$, no current flows, and the Zener diode prevents unnecessary energy dissipation. The current through the Zener diode when the cell voltage exceeds the Zener voltage V_z is given in (7).

3) Switched Shunt Resistor Topology

The switch-resistor topology allows for bypassing the current during charging or discharging to partially discharge the cell. A control mechanism is required to monitor the voltage and manage the switching of the transistor, as shown in Fig. 4(h). Table II shows the comparison of various CB techniques.

III. CYBERSECURITY THREATS IN EVS

EVs are equipped with hardware and software. It is necessary to protect both from cyber threats. Hardware components consist of sensors such as voltage, current, temperature, lidar, cameras, pressure sensors, airbags, and ignition [38]. EVs utilize microcontrollers such as STM32, DSP, or FPGA for fast control of the vehicle. Below is a detailed list of hardware components used in EVs, as shown in Fig. 5(a). BMS comprises four distinct layers: the network layer, database layer, software layer, and hardware layer. BMS controls battery charging, discharging, and temperature management and is vulnerable to attack if firmware is tampered with or sensors are manipulated, leading to battery failures or safety risks. Components like FPGA chips and STM32 or DSP microcontrollers are integral to controlling. Various vehicle systems utilize CAN communication to the ECU, including the motor controllers, regenerative braking, and charging units. If these hardware elements are compromised through physical tampering, reprogramming, or side-channel attacks, it could lead to unpredictable motor behaviour, compromised battery health, or even failure of critical safety systems. For example, if the charging current reference value in the onboard charge controller is changed, it can damage the battery. Fig. 5(b) illustrates the security layers and various cyberattacks.

Detecting and mitigating threats to CPS in EVs is crucial

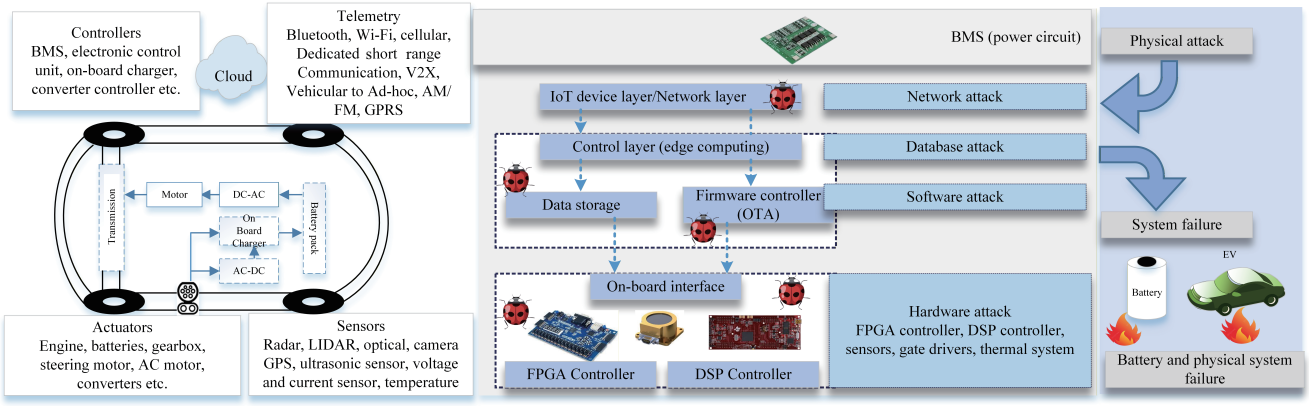


Fig. 5. Overview of critical EV components vulnerable to cyberattacks and security layers of BMS and various cyberattacks. (a) Electric vehicle components under attack. (b) Layout of security layers of BMS and various cyberattacks.

due to the increasing complexity and connectivity of modern EVs, which integrate both cyber and physical components. To effectively detect threats, continuous monitoring and anomaly detection are needed. Several studies have been done related to attack detection in cyber-physical systems. For example, attack trees [48], Petri nets [49], and game theory [50]. Additionally, communication networks, including the CAN bus, need to be monitored for unauthorized access or malicious data injections. Intrusion detection systems can be deployed in both embedded systems and vehicle communication networks to detect potential cyber intrusions. At the hardware level, tamper detection mechanisms and fault detection and diagnostics algorithms can be used to identify physical threats. Moreover, adopting strong user authentication protocols, such as multi-factor authentication (MFA), and employing role-based access control (RBAC) ensures that only authorized EV owners can access the vehicle. In [51], vulnerabilities in EV powertrains are investigated using an OPAL-RT real-time simulator and a hardware-in-the-loop (HIL) controller. In [38], the authors examine the denial of charge (DoC) attack in plug-in EVs, which are connected to EVSE. The study was conducted on two types of attacks on BMS data, overcharging and denial of charging through EVSE. An attacker can manipulate the actuated current and voltage.

Firmware in the BMS can be accessed and modified both remotely and locally. It includes operating systems, source code (including algorithms for BMS and communication protocols), and related components. Updates and maintenance of this firmware are often handled by authorized users or vendors, sometimes facilitated by over-the-air update capabilities. However, this accessibility also introduces potential security vulnerabilities within the BMS firmware [26]. Most of the firmware is considered risky because it is not digitally encrypted for the microcontrollers or FPGA [52]. The integrated circuit makers do not cryptographically sign the firmware incorporated in their systems, nor do they implement authentication mechanisms in their products. Moreover, current BMS software/firmware lacks capabilities for detecting malware or unauthorized code modifications.

The potential for unauthorized access and modification via malware (such as Trojans, viruses, and botnet infections exemplified by Stuxnet, Mirai, and ransomware) exists, whether through internet connections or physical access to the BMS. Cyberattacks may introduce malicious software or alter source code, damaging hardware components such as switches and sensors, while also increasing the degradation of LIBs and leading to severe consequences. In extreme cases, the batteries may overheat, catch fire, or even explode.

EVs comprise embedded systems such as control ECUs, infotainment units, telemetry modules, on-board chargers, and safety-critical components, including BMS. While many of these devices are protected by manufacturer-exclusive access, some remain physically reachable and therefore vulnerable. Attackers with the ability to gain access to the CAN bus and hack the BMS or DSP/FPGA for changing the reference values [53]. Additionally, the on-board diagnostics (OBD) interface provides access to critical vehicle information and diagnostic data, making it a high-value target for unauthorized exploitation if not adequately protected. Because such attacks require specialized knowledge and tools and because many ECUs incorporate redundancy or backup modules, both the probability and impact of compromising these embedded systems are considered medium, resulting in a medium overall risk. Fig. 6(a) contains the power and control circuit for the onboard charger used in EVs. It is controlled by the DSP or FPGA controller, which is connected to the CAN bus to communicate with the main controller and the BMS circuit. The controller is used to control the onboard inverter and DC-DC converter in a closed loop. An attacker can attack the controller through the CAN bus and manipulate the actual set of values [26].

FPGA logic enables continuous real-time monitoring of critical signals such as gate pulses, sensor feedback, communication interfaces (CAN, PLC, Ethernet), and pulse width modulation (PWM) patterns. It is required to protect the firmware of the controllers by anti-tampering techniques like encryption of

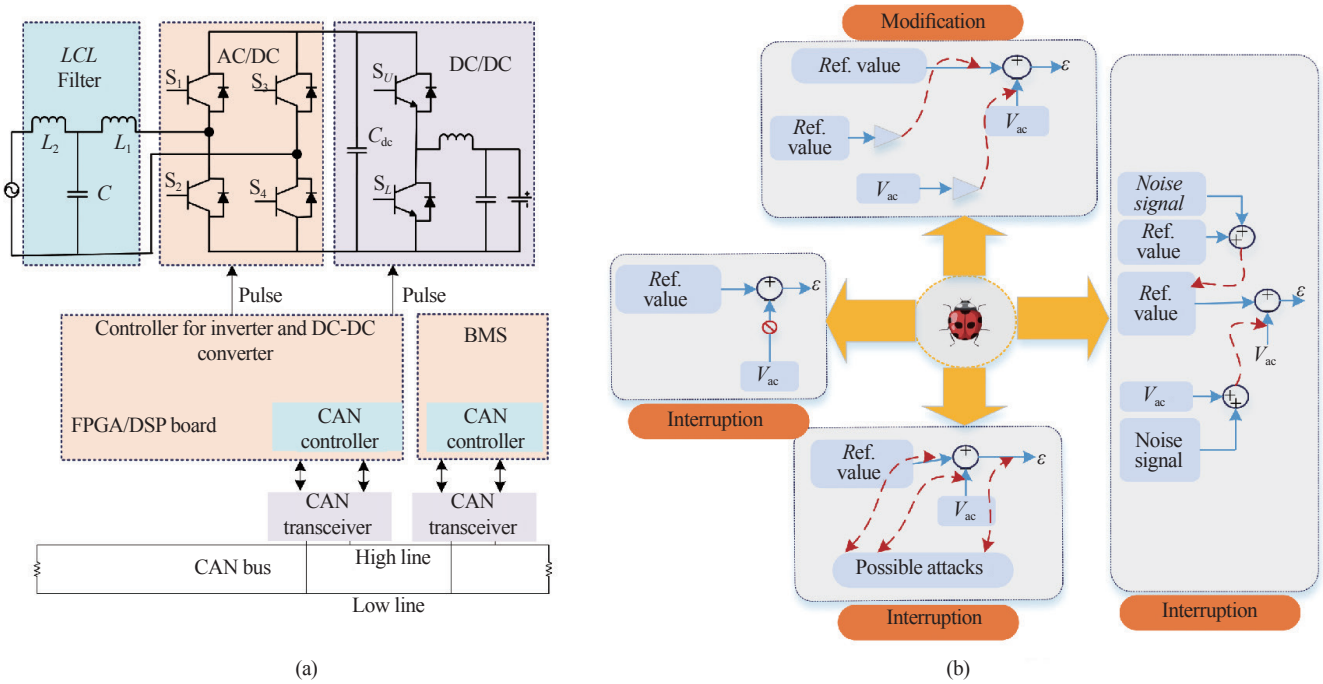


Fig. 6. The block diagram of (a) an on-board charger of an EV with CAN bus communication and (b) major cyberattacks related to the inverter and converter of an on-board charger.

firmware. A method of code swapping and cloning firmware to protect it from attack is discussed in [54]. Cybersecurity issues related to converters and controllers, like modification, interference, intrusion, and interception attacks. A digital circuit is used to detect the attack in PWM pulses of the controller. Moreover, software- and hardware-based (controller) attack mitigation techniques are discussed in [55]. In [56], the authors focus on attacks that tamper with FPGA configuration bitstreams, examining vendor protection mechanisms, methods attackers use to bypass them, and types of bitstream modification attacks.

Fig. 6(b) shows the major cybersecurity attacks on the controller of the onboard charger. In order to utilize the BMS and to secure the EV from cybersecurity, various standards are provided to ensure the cybersecurity and safe operation of the BMS, as shown in Table III [57]. Table IV provides a literature survey on cyberattack detection and mitigation techniques in EVs.

A. Controller Area Network (CAN)

It allows communication between sensors, actuators, controllers, and ECUs in EVs. There are two types of CAN communication: high-speed CAN transfers data up to 1 MBPS, and low-speed CAN transfers data up to 10–125 kbps. The system consists of a USB-CAN smart card equipped with a freescale 16-bit microcontroller and a Phillips semiconductor USB interface module [63]. It offers features, including support for both 11-bit and 29-bit CAN identifiers, time-stamped CAN messages with 10-microsecond resolution, and large onboard RAM for message buffering. The priority is inversely proportional to the message ID value, a lower message ID corresponds to a higher priority for gaining access to the bus. If two nodes attempt to transmit data at the same time, the node with the lower message ID will transmit first due to its higher priority. This process is known as message arbitration. For example, if three nodes (first node: 11001101111, second node: 110011111111) try to transmit simultaneously, the node with the lowest ID will gain bus access and transmit its message first, as shown in Fig. 7(a). Fig. 7(b) shows the different ECUs connected to the CAN bus.

B. Inter-Integrated Circuit (I2C)

The I2C protocol, created by Philips, provides a two-wire interface consisting of a clock line (SCL) and a data line (SDA). The controller generates the clock signal and initiates communication, while the target replies to the controller's commands. The controller starts communication by sending a start condition, followed by a 7-bit address and a read/write bit. The read/write bit tells the controller whether the operation will be a write (0) or a read (1). Should the target node exist and be responsive, it confirms the address with an ACK (active low). A start situation is signified by a high-to-low transition of SDA while SCL is high, and a halt state is denoted by a low-to-high transition of SDA with SCL remaining high. All other data exchanges transpire when SCL is in a low state. It is used in EVs for displays, BMS, ECU, converters, sensors, motors, and light communication [61].

C. Serial Peripheral Interface (SPI)

SPI is a synchronous serial communication protocol used to facilitate high-speed data transfer between microcontrollers and peripheral devices. It operates in full-duplex mode, allowing data to be sent and received simultaneously, which makes it ideal for time-sensitive applications. It is used in BMS and

TABLE III
VARIOUS STANDARDS UTILIZED FOR CYBERSECURITY AND BMS OF EVS

Standard	Purpose
ISO/SAE 21434	Defines the cybersecurity engineering process for road vehicles, covering threat analysis, risk assessment, and secure lifecycle management.
SAE J3061	Provides a framework for integrating cybersecurity into the vehicle development lifecycle. It defines processes for threat analysis, risk assessment, and designing secure automotive systems, complementing ISO/SAE 21434.
ISO 11898-1 /11898-2	Specifies the CAN communication protocols used in the BMS of EVs.
SAE J1939 [58]	Defines communication standards for heavy-duty vehicles and commercial buses. It provides a standardized CAN framework for exchanging data between vehicle components such as the BMS, traction motor controller, inverter, DC/DC converter, and thermal systems.
SAE J2464	A comprehensive set of electrical, mechanical, and thermal abuse tests designed to evaluate how EV battery systems respond to extreme or fault conditions such as overcharge, short circuit, crush, penetration, and fire exposure.
IEC 62443	Provides a framework for industrial automation and control systems security, relevant for automotive manufacturing and connected systems.
NIST SP 800 -95 [59]	Modern EVs rely on connected services, many of which use SOAP/REST APIs, cloud web services, and service-oriented architectures. NIST SP 800-95 focuses on securing web service communication.
UL 2580	Discuss the electrical, mechanical, environmental, and functional safety of EV battery systems.
IEC 61850	Standard for communication networks and systems in utility automation, relevant to smart charging and vehicle-to-grid interactions.
UN R155	This standard defines cybersecurity obligations for contemporary road vehicles, mandating that manufacturers establish a comprehensive cybersecurity management system encompassing threat assessment, implementation of technical safeguards, continuous monitoring, incident handling, and secure a software update process.
OCPP	OCPP is a communication protocol used to connect EV charging stations with central management systems. It helps in monitoring, controlling, and managing chargers, regardless of the manufacturer or charging network. OCPP supports essential functions such as starting and stopping charging sessions, user authentication, smart charging, load balancing, firmware updates, fault reporting, and billing. Modern versions of OCPP, such as 1.6 J, use JSON over WebSocket.

TABLE IV
LITERATURE SURVEY ON CYBERATTACKS DETECTION AND MITIGATION TECHNIQUES IN EVS

Ref./Year	Insight	Algorithm used	Attack type
[38]2020	This paper has an analysis of a denial-of-charge attack to damage the battery by overcharging. This attack is detected using two algorithms: a static detector by measuring the static variable. Another is dynamic variables.	The attack detector algorithm is used in EVSE and EV which are connected through protected Wi-Fi communication. The paper proposes a filter-based design approach for the dynamic detector.	DoC
[51]2021	This paper focuses on cyberattack identification algorithms to mitigate cyberattacks in CPS. The models are validated on the powertrain control security.	LR, ANN, convolutional neural network	False data injection
[60]2023	The paper proposes a strategy for detecting cyberattacks on PEVs during charging, using complete ensemble empirical mode decomposition with adaptive noise and a broad learning system.	CEEMDAN and BLS	False data injection
[61]2021	This paper discusses the cyberattack on sensor data and distributed generation units and their sensors. To create robust training datasets, bootstrap sampling is used to generate separate subsets for each base model. This ensures that the training data for each model is diverse and can effectively capture various aspects of the signals. The method then incorporates selective ensemble learning, using a combination of enhanced weighted voting and class-specific thresholds.	Hilbert-Huang transform with deep learning techniques to enhance the detection of various cyberattacks.	False data injection technique
[62]2020	The authors propose a novel approach using physics-guided machine learning to detect cyberattacks on EVs across varying driving scenarios. The OPAL-RT-based test bed is simulated.	Physics-guided machine learning, machine learning-based classifier.	DoS and false data injection

I2C-based sensors. The protocol's high-speed communication and minimal hardware requirements make it an excellent choice for EVs [14].

D. Modbus

It is used to connect the EV charging stations to the main server. The Modbus protocol follows a master-slave communication model, where one device initiates communication, and the other devices respond to the master's requests. The master device can query, read, and write to the slave devices, but slaves cannot initiate communication [64].

E. Bluetooth Low Energy (BLE)

Bluetooth technology, overseen by the Bluetooth Special

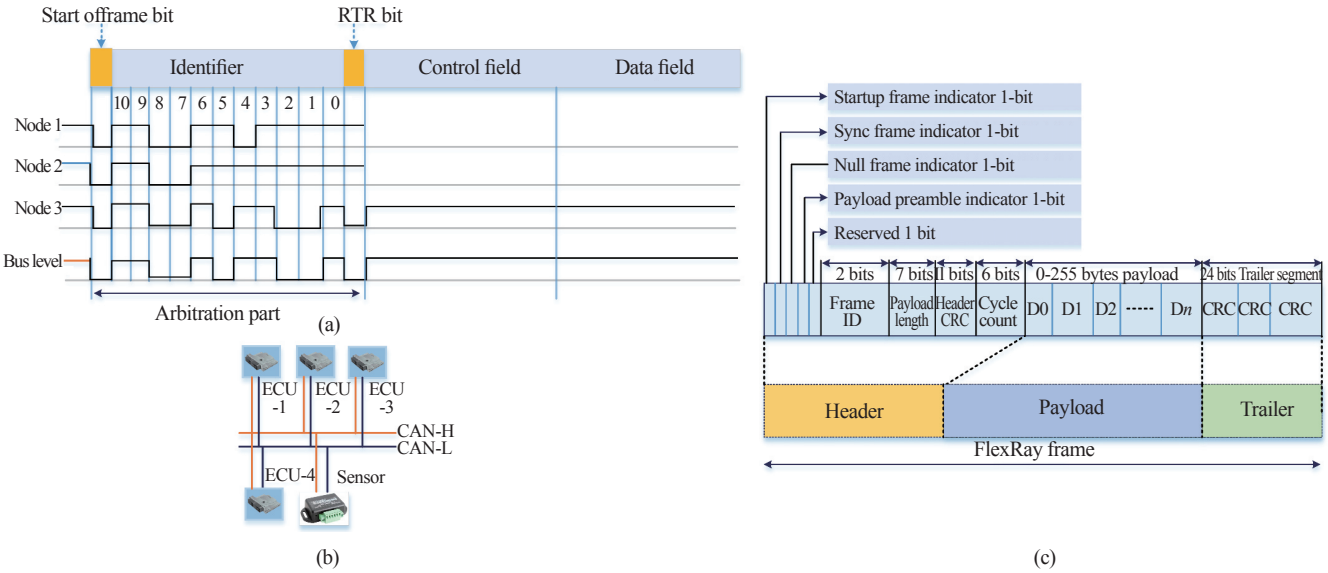


Fig. 7. Communication protocols used in electric vehicle networks. (a) Frame used in CAN-bus communication. (b) Layout of CAN communication. (c) Frame used in FlexRay communication.

Interest Group (SIG), has evolved into a substantial standard for wireless communication for short-range applications. Bluetooth SIG introduced BLE, a power-efficient variant of the traditional Bluetooth protocol. Despite operating in the same 2.4 GHz ISM band as bluetooth classic, BLE is backwards-incompatible and offers different communication methods, including one-to-many communication rather than the one-to-one connection in bluetooth classic [65].

F. ZigBee

ZigBee operates within the industrial, scientific, and medical radio frequency spectrum, primarily employing the 2.4-GHz range for applications including home automation. This band receives worldwide endorsement, employing sub-GHz frequencies (902–928 MHz in North America, 868–870 MHz in Europe, and 779–787 MHz in China) for commercial metering and medical apparatus across diverse regions. ZigBee data rates range from 20 kbit/s in the sub-GHz spectrum to 250 kbit/s in the 2.4 GHz region. The ZigBee standard utilizes the IEEE 802.15.4 physical and media access control layers for low-rate wireless personal area networks.

G. FlexRay

It is designed to be faster and more reliable than its predecessors, CAN and LIN. FlexRay is network-flexible by supporting multiple topologies, such as bus, star, and hybrid configurations. In the star topology, a central active node connects to all other nodes, functioning similarly to a hub in an Ethernet network [66]. This configuration allows the network to cover longer distances and enables segmentation, ensuring that the failure of one segment does not disrupt the entire network. It has three different topologies: (a) Multi-drop bus, a simple network with one trunk and multiple ECUs. Each node has a fixed spot for data transmission. (b) Star network: Nodes are connected to a central active node, providing higher reliability and better noise immunity. (c) Hybrid topology: It is the combination of a multi-drop and a star topology. A FlexRay frame consists of three main segments, as shown in Fig. 7(c). These are header, payload, and trailer. The detail of each segment is given below.

1) Header: It is 5 bytes long. It is divided into various fields. i) Status bits: These bits are used to represent the state of the frame. They help in error detection and frame management. ii) Frame ID: It determines the position of the frame in the communication cycle and helps prioritize event-driven messages. iii) Payload length: This parameter indicates the length of the payload. It defines how much data the payload will contain. iv) Header cyclic redundancy check (CRC) : The CRC is used for error detection in the header.

2) Payload: The payload contains the actual data being transmitted. The length of the payload can be up to 127 words.

3) Trailer: The Trailer segment is used for error detection. The trailer contains three 8-bit CRCs to ensure that the frame is received without errors during transmission.

IV. BMS and SoC Estimation Techniques

BMSs play a vital role in ensuring the safe and efficient operation of LIBs. Beyond basic monitoring, the BMS controls charging, discharging, thermal behaviour, and protection mechanisms. BMS is an essential component in LIBs. A key parameter monitored by BMS is the C-rate, which determines how quickly a battery can be charged or discharged relative to its rated capacity. The C-rate of the battery pack depends on the battery chemistry, temperature, and battery SoC. SoC estimation using a particle filter with 0.63% MSE is discussed in [67]. Accurate state estimation is critical to optimizing battery performance. A literature survey for SoC parameter estimation using various techniques is given in Table V.

Coulomb counting is the conventional method to find the SoC of a battery [69]. The following equation defines the SoC:

TABLE V
LITERATURE SURVEY FOR SOC PARAMETER ESTIMATION USING VARIOUS TECHNIQUES

Ref./Year	Finding	Algorithm used
[67]2023	The mean square error is 0.63% in HIPF.	H-infinity particle filter
[68]2018	The SoC estimation is done using the H-filtering method. The H-filtering is compared with the extended KF estimation to validate the proposed results. The SoC is estimated using the battery voltage with varying temperatures of 20° and 40°.	H-infinity filtering and the extended KF are used.
[17]2013	The accuracy of the SVM-based model is 6%. The test is carried out on a 60 Ah LIB.	SVM

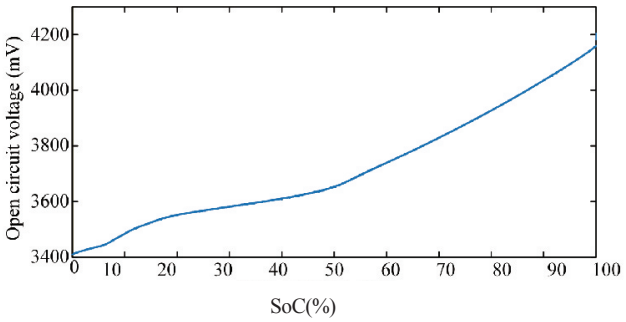


Fig. 8. OCV versus SoC curve for Coulomb counting.

$$SoC(t) = SoC(0) + \frac{\eta_i}{C_n}\int_0^t i(t)\mathrm{d}t \tag{8}$$

where $SoC(t)$ is the SoC at time t, $SoC(0)$ is the initial SoC, and η_i is the Coulomb efficiency. C_n is the battery's nominal capacity, and it is the current, with discharge current taken as positive. From (1), it is concluded that the SoC is determined by the integration of current over time. Fig. 8 shows the OCV versus SoC curve for the coulomb counting method for the dataset taken from [70].

A. Model-Based Approaches

ECMs: ECMs use model-based methods for estimating battery states such as SoC. These models simplify the complex electrochemical processes occurring within a battery to electrical quantities, such as resistors, capacitors, and voltage sources [71]. The third-order RC equivalent circuit can be used to predict the SoC using ECMs. Emanuele et al. [72] depict SoC estimation of LIB using electrochemical impedance spectroscopy (EIS), ECM, and ML. EIS data was collected from four lithium-ion cells across ten SoC levels using a prototype measurement system. The best performance is achieved using ECM parameters with k-NN, with 93.9% accuracy.

Physics-based models (PBMs): The classical electrochemical models are based on the physical and chemical principles that govern battery processes, including ion transport, electrochemical reactions, and thermodynamics. Consequently, PBMs are commonly working for better estimation of battery states, such as SoC, degradation, and failure. The electrochemical model, which is the most widely used physics-based model for LIBs, is based on the Pseudo Two-Dimensional (P2D) framework, also known as the Doyle-Fuller-Newman model. This model defines the flow of lithium ions between the anode and cathode through the electrolyte, the electrochemical reactions at the electrodes, and the changes in concentration and potential within the cell [73]. The equations contain the Nernst-Planck equation for ion transport, Butler-Volmer kinetics for reaction rates, and mass and charge conservation laws.

$$\begin{cases} \mathrm{LiMO_2} \rightleftharpoons \mathrm{Li_{1-X}MO_2} + X\mathrm{Li^+} + \mathrm{Xe^-} \\ \mathrm{C} + \mathrm{Li^+} + \mathrm{Xe^-} \rightleftharpoons \mathrm{Li_X C} \\ \mathrm{LiMO_2} + C \rightleftharpoons \mathrm{Li_X C} + \mathrm{Li_X MO_2} \end{cases} \tag{9}$$

B. Data-Driven Methods

These methods can identify patterns and correlations without needing an in-depth understanding of the battery chemistry. These methods are explained below:

1) SVMs

SVMs are powerful supervised learning algorithms used for estimating the SoC of batteries. For SoC estimation, SVMs utilize various input features, including voltage, current, temperature, and charge/discharge cycles. The model is trained on historical data, employing hyperparameter optimization techniques like grid search or cross-validation to find the best settings. Once trained, the SVM model predicts the SoC for new data by identifying the optimal hyperplane that separates different states within the feature space [17].

The input features (X) can be written as

$$X = \{V(t), I(t), T(t), t\} \tag{10}$$

where voltage (V), current (I), temperature (T), and time (t) are represented as a vector of features, the output vector is $y = SoC(t)$. The input features are mapped to the output SoC. The SVM aims to find a function $f(X) = w^{\mathrm{T}}X + b$.

where w is the weight vector, b is the bias term, and X is the input feature vector. Optimization of the weight factor of the function $f(X)$. Minimize the following objective function that combines a loss function and a regularization term.

$$\min_{w,b,\xi,\xi^*} \left\{ \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{N}(\xi_i + \xi_i^*) \right\} \tag{11}$$

Subject to $y_i - (w^T X_i + b) \leqslant \epsilon + \xi_i$,

$$(w^T X_i + b) - y_i \leqslant \epsilon + \xi_i^*, \xi_i, \xi_i^* \geqslant 0 \tag{12}$$

where $1/2\ \|w\|^2$, is the regularization term to prevent overfitting, ξ and ξ^* are the slack variables to handle data points that fall outside the ϵ insensitive zone, and C, a hyperparameter.

2) ANNs

For SoC estimation, the ANN model requires a real-time data set or a simulated data set to train the ANN model. It takes inputs: voltage, current, and temperature. The number of hidden neurons depend on the complexity of the model. The

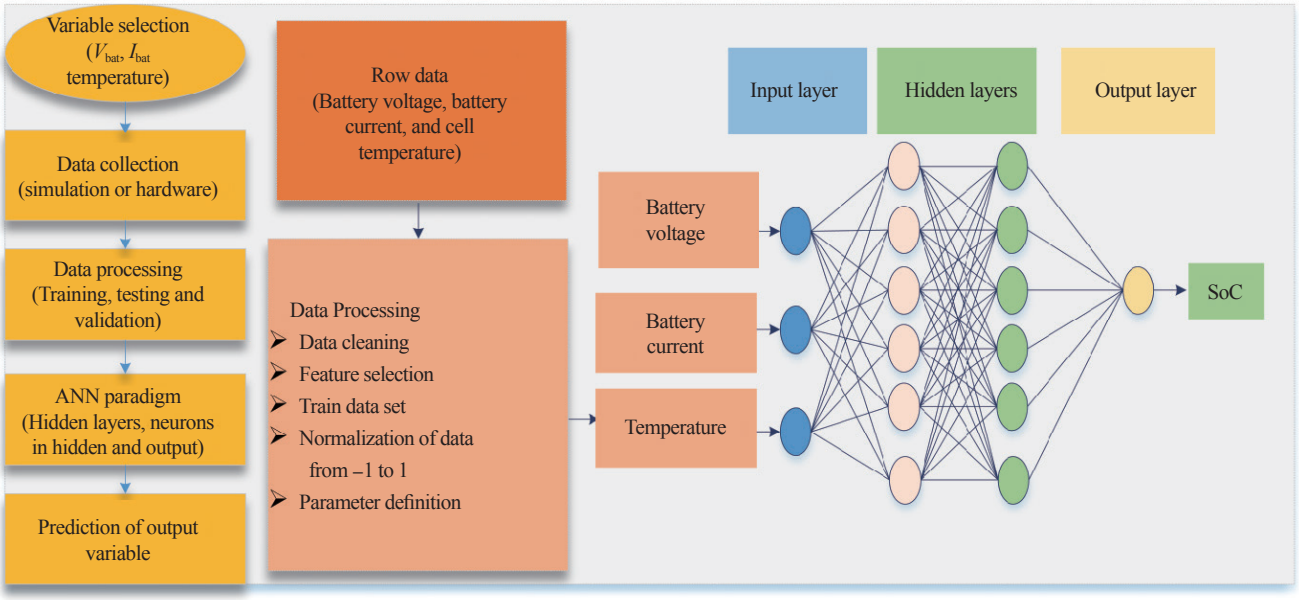


Fig. 9. SoC estimation using artificial neural networks. (a) Flow chart of the ANN for SoC estimation and. (b) ANN architecture for SoC estimation.

training process involves adjusting the weights of the network through backpropagation, where the error between predicted and actual SoC values is minimized. In [74], a comparison of an ANN and a KF-based model is tested on a LIB of 2.6 Ah and 3.8 V nominal voltage. ANN is used to estimate the SoC of $LiFePO_4$ [75]. The SoC and capacity measurements for two identical 3.6-V/16.5-Ah LIBs were performed. After 2000 cycles, the SoC error was 0.1613 [76].

The performance of the trained model is measured using RMSE and correlation coefficient (R^2).

$$y = f\left(\sum_{i=0}^{n} w_i x_i + \text{bias}\right) \tag{13}$$

where f is the tangent activation function, w_i is the weight corresponding to the neuron, and x_i is the output of the previous layer, and bias is the offset for neurons

$$f(x) = \tanh x = \frac{1}{1+e^{-x}} \tag{14}$$

Fig. 9(a) shows the flowchart of the neural network used to estimate SoC. Fig. 9(b) shows the layout of the implementation of the neural network to estimate SoC.

The implementation of an ANN-based SoC estimator requires storing the software as embedded code in nonvolatile memory, which the microprocessor executes during each sampling period. While ANNs can be implemented using DSPs, microcontrollers, or FPGAs, FPGAs have gained significant traction recently due to their reconfigurable architecture, low cost, and availability for ANN applications [76], [77].

3) DNN

DNN-based SoC estimation refers to using deep learning models to predict a battery's SoC from measurable signals such as voltage, current, temperature, and historical operating data. In [78], the authors present HIL system designed specifically for battery control applications, machine learning (ML), and AI in BMS. In [79], ODiMO is a hardware-aware optimization framework that performs DNN layer partitioning across available computer units during training. By developing parallel execution while accounting for accuracy implications, ODiMO identifies mappings that balance inference latency or energy against model performance. Experiments on CIFAR-10, CIFAR-100, and ImageNet, using the DIANA and Darkside heterogeneous SoCs, show that ODiMO achieves up to 8 times latency reduction and up to 50.8 times energy improvement with negligible accuracy loss (< 0.3%), compared to heuristic mapping strategies. This work highlights the importance of hardware-aware neural network optimization for efficient edge deployment. This method is discussed in [20]. The authors implement a DNN-based SoC estimation algorithm on Li-polymer batteries. The DNN can estimate the SoC once the charging data has been collected. The input sequence of data is sampled within the window. This enables real-time SoC estimation by continuously updating the recent element of the input sequence after initializing it with a starting set of data. However, it's important to note that the DNN's SoC estimates at two consecutive moments, $y(t)$ and $y(t-1)$, are independent, as the DNN directly links current and voltage signals with SoC values. At time step t, given an input $x(t)$, the hidden state $h(t)$ is updated as (14).

$$h(t) = \sigma[W_h \cdot h(t-1) + W_x \cdot x(t) + b] \tag{15}$$

where $h(t)$ is the hidden state at time t, $h(t-1)$ is the hidden state at the previous time, $x(t)$ is the input at time t, W_h and W_x are weight matrices that determine the last hidden states and current states, σ is the activation function, and b is the bias

term. The output of the network is calculated as

$$y(t) = W_y \cdot h(t) + b_y \tag{16}$$

C. Statistical Methods

It works on the principles of Bayesian estimation, providing optimal state estimates in a linear dynamic system degraded by Gaussian noise. The Kalman filter (KF) consists of two steps: prediction and update. In the prediction phase, the filter uses a mathematical model of the battery dynamics to estimate the next state based on previous states and inputs, such as voltage, current, and temperature. The predicted state is accompanied by an estimate of the uncertainty, represented by a covariance matrix. In the update phase, the KF includes new measurements to refine its predictions. By calculating a Kalman gain, which balances the trust between the model predictions and the observed measurements, the filter adjusts the state estimates and reduces the uncertainty in the estimation. SoC estimation can be done by letting the state $x(k)$ represent the SoC of a battery, which changes over time due to charging and discharging processes. It is calculated as a state equation:

$$x(k) = Ax(k-1) + Bu(k-1) + w(k-1) \tag{17}$$

where A is the system transition matrix, B is the input matrix, $u(k-1)$ is the control input, $w(k-1)$ is the process noise that accounts for any model inaccuracies or other disturbances affecting the system, and Q_f is the process noise covariance matrix. The measurement equation is written as

$$y(k) = Hx(k) + v(k) \tag{18}$$

Here, $y(k)$ is the measurement of input quantities, H is the measurement matrix that links the state $x(k)$ to the observable measurement $y(k)$, and $v(k)$ is the measurement noise, assumed to be Gaussian with covariance R_f. The prediction of SoC is calculated using the equation given below:

$$\bar{x}(k) = Ax(k-1) + Bu(k-1) \tag{19}$$

The prediction of SoC at time instant k is done based on the previous state and control input. The prediction error covariance is calculated by updating it based on the system dynamics and process noise, is calculated as

$$\bar{P}(k) = AP(k-1)A^T + Q_f \tag{20}$$

The Kalman gain determines the weight given to the new measurement. It is calculated as

$$K(k) = \bar{P}(k)H^T[H\bar{P}(k)H^T + R_f]^{-1} \tag{21}$$

The updated states are calculated using:

$$x(k) = \bar{x}(k) + K(k)[y(k) - H\bar{x}(k)] \tag{22}$$

The covariance error is updated using:

$$P(k) = \bar{P}(k) - K(k)H\bar{P}(k) \tag{23}$$

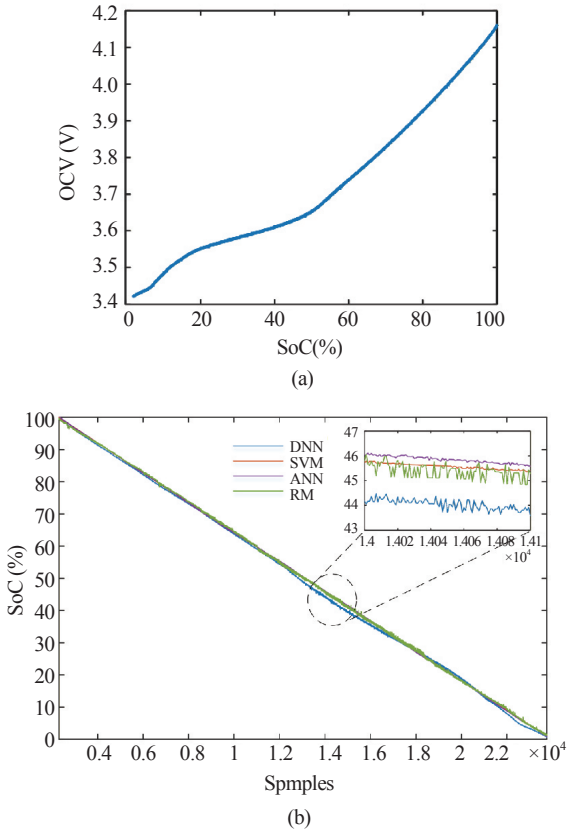


Fig. 10. The curve plotted from actual data. (a) OCV vs. SoC (%) and (b) SoC estimation using various methods.

TABLE VI
RMSE AND MEAN ABSOLUTE ERROR (MAE) PERCENTAGE ERROR FOR VARIOUS SOC ESTIMATIONS

Error	DNN	SVM	KF	ANN	RM
RMSE/%	0.6	0.42	8.6	0.1	0.41
MAE/%	0.44	0.05	7	0.08	0.28

After updating the state and covariance, increment the time step $k = k+1$ and repeat the prediction and update steps. Fig. 10(a) shows OCV curve of an 18650 battery with a 3.6 V nominal voltage. Fig. 10(b) shows the comparison of various SoC estimations. The dataset used for SoC estimation is utilized from [70]. Analysis of various methods is provided in Table VI. It shows the ANN method has 0.1% RMSE compared to other methods. Random forest (RM) and SVM show equal RMSE. Pros and cons of SoC estimation techniques are given in Table VII. A comparison of computational complexity and hardware requirements for ANN and DNN is provided in Table VIII.

The literature review of various SoC estimation techniques is provided in Table IX.

V. APPLICATION OF BLOCKCHAIN TECHNOLOGY

As EVs increasingly rely on BMS, the cybersecurity of BMS, controllers, and data integrity has become a critical

TABLE VII
PROS AND CONS OF VARIOUS SOC ESTIMATION TECHNIQUES

Model type	Pros.	Cons.
Empirical model	Computationally efficient; simple expression	Limited capability in describing the terminal voltage
Equivalent circuit model	Widely used for SoC estimation; easily understandable	Parameter identification is complex
Electrochemical model	High accuracy in voltage calculation	Requires prior battery knowledge
Data-driven model	High accuracy in voltage calculation	Difficult to collect the training dataset

TABLE VIII
COMPARISON OF COMPUTATIONAL COMPLEXITY AND HARDWARE REQUIREMENTS FOR ANN AND DNN

Algorithm	Computational complexity	Hardware requirements	Memory usage	Real-world applicability	Implementation challenges
ANN [76]	Moderate	FPGA, DSP, and microcontroller	Low to moderate	Used in an EV battery pack	Moderate
DNN [78], [79]	High	CPU, GPU, FPGA, and STM32	High	SoC estimation for LIBs	High

TABLE IX
LITERATURE REVIEW OF VARIOUS SOC ESTIMATION TECHNIQUES

Ref./Year	Category	Findings	RMSE	MAE	Accuracy
[69]2018	Coulomb counting	Accuracy is lower because of the current sensor error and the accumulation of error in the current measurement. Providing an initial SoC value may not be accurate. Nonlinear filters are executed on a Xilinx Zynq XC7Z020 via a model-based design methodology in Simulink.	2%	0.065	Less
[67]2023	H-infinity filter	The study is conducted on retired Li-ion batteries (BAIC EV150 under FUDS and DST cycles) with an 80% remaining capacity. The SoC estimation is done by enhancing the H-infinity filter with an H-infinity particle filter.	–	0.63%	–
[72]2023	ECMs	EIS data is combined with ML and EMCs for SoC estimation. The study of ML-based SoC estimation techniques. Three algorithms were tested: k-NN, Gaussian Naïve Bayes, and linear support vector classifier.	–	–	93.9%
[80]2014	OCV	FUDS and DST drive cycles are used for testing. $LiFePO_4$ (3.3 V, 1.1 Ah) is used for testing.	0.0095/25°	0.0080/25°	–
[69]2018	ANN and H-infinity filter	The particle filter (PF) with the lowest MAE balances accuracy and execution time well, as does the H-infinity filter. SR-UKF and SR-CDKF have a fast response. The H-filter execution time is 0.034674 ms. The evaluation of seven distinct nonlinear filters for SoC estimation demonstrates the precision of the MBMs.	–	0.0065 (H-infinity)	–
[81]2021	SVM	The comparable circuit network is utilized to gather real-time data. A Recursive Least Squares algorithm associated with the SoC of the battery, utilizing a Support Vector Machine classifier to predict the SoC. A lithium sulfur cell (2.4 V, 19 Ah, 3C) is utilized for testing purposes.	<3%	<3%	93%/25°
[74]2019	ANN and UKF	A 2.6 Ah Samsung AA1F329TS/2-B battery, with a nominal voltage of 3.8 V, is used for testing. The ANN model contains 9 neurons in hidden layers.	1.90%	0.5% (NN) and 4.5% (UKF)	–
[82]2020	DNN	Proposed the four-hidden-layer DNN training model. 2.0 Ah, 18650NMC battery is used for testing on DST, FUDS, BJDST, and US06 drive cycles.	3.68%	0.13%	–
[83]2025	KF	Develop an adaptive multi-model KF that adjusts measurement parameters based on OCV error signs, selecting the optimal filter using predicted voltage probabilities.	<0.03	11.85%	High
[84]2019	KF, UKF	Reviews the family of KF methods to predict the SoC in LIBs.	–	–	–

concern of security. Moreover, the functions of BMS, such as SoC estimation, protection, and CB, are important for the safe operation of EVs. IoT devices, cloud platforms, and communication networks integrate with modern BMS architectures, exposing them to cyber-physical threats [22]. To address these vulnerabilities, blockchain provides decentralized, tamper-resistant mechanisms for securing BMS data. This section introduces the use of blockchain as a secure technology for BMS communication and storing BMS data after anomaly detection. An 11.1 V, 4400 mAh LIB is used for analysis and data storage on the blockchain after anomaly detection.

Blockchain technology, with decentralized and immutable properties, can enhance the security of BMS. Hyperledger Fabric is a private and permissioned blockchain platform developed by IBM. BMS applications provide access control and a consensus mechanism in creating blockchain ledgers. Further-

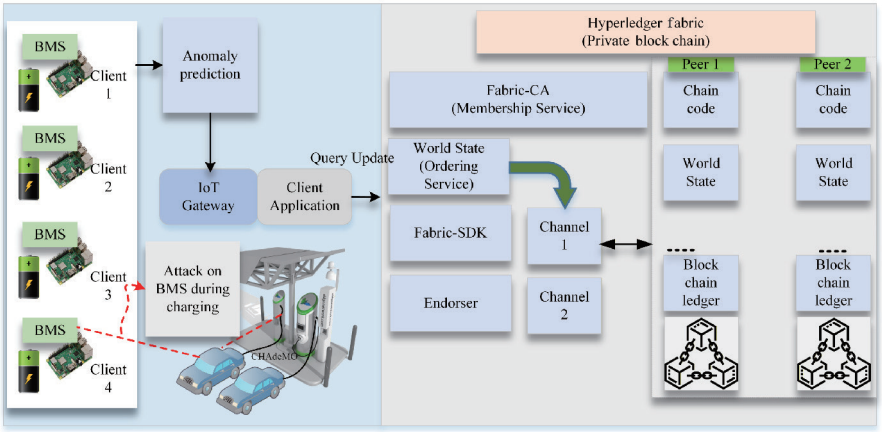
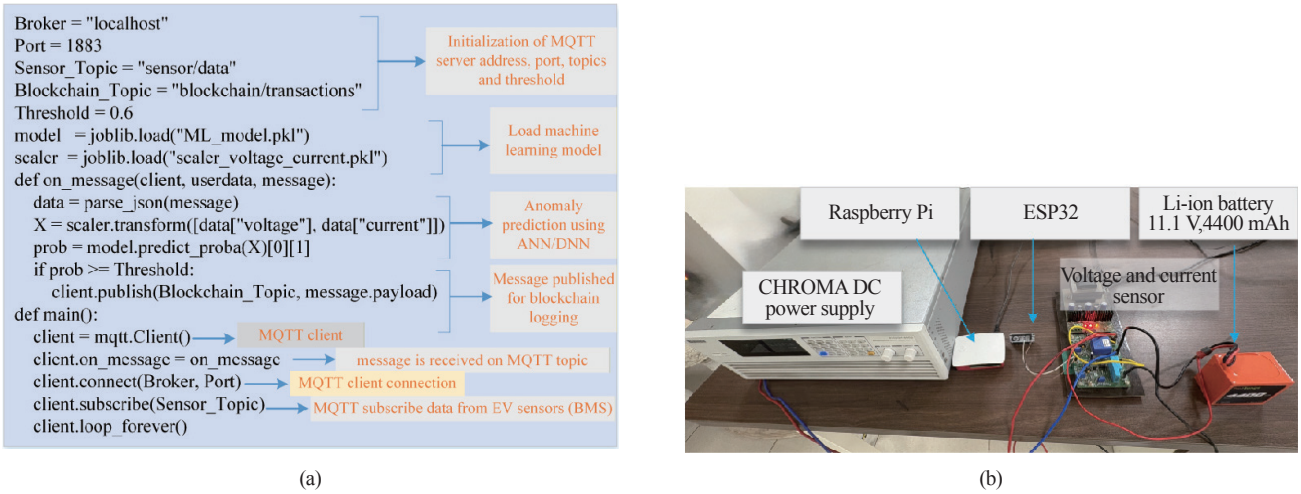


Fig. 11. Illustration of a Fabric network with anomaly detection and IoT.



(a) (b)

Fig. 12. Blackchain-based anomaly detection and validation setup. (a) Integration of the detection module and MQTT for transmitting anomaly data to the blockchain server and (b) hardware prototype used for blockchain validation.

more, Fabric supports smart contracts, known as chaincode, which enable business logic to be executed on the blockchain. A command-line interface or a client application controls the chain code. Fig. 11 shows the layout of the fabric-based implementation of blockchain using a client application [25]. The fabric network is installed on Linux; each node of the IoT client is enrolled through Fabric-CA, and a certificate is issued to the client. Once the client is authorized, the IoT client can interact with the blockchain by executing a smart contract through a client application. It communicates with peer nodes in the blockchain network. This model is implemented in two organizations and four peers in the networks, using a test network of Fabric.

The data generated by the battery modules (anomaly) is sent to endorsement peers for validation, and after validation, it is sent to the orderer peer for sequencing into blocks. These blocks are then distributed to the peer nodes and added to the blockchain ledger. Data is stored if an anomaly is detected in the BMS circuit during charging. Fig. 12(a) shows the integration of machine learning algorithms for anomaly detection in BMS data. If an anomaly is detected by a machine learning algorithm, it publishes the anomaly data to an MQTT topic, which is subscribed to by a client application to communicate with a smart contract. The application receives real-time data from the BMS communication module, which is transmitted by IoT devices (ESP32/Raspberry Pi). Fig. 12(b) shows the hardware prototype used to validate the proposed architecture. A personal computer (i9, 32GB RAM, 16GB RTX3050) is utilized to install the Fabric network. Fig. 13 shows the layout of the client application, which is integrated into the Fabric network to communicate with a smart contract or ledger. This application is connected to an MQTT server to receive the anomaly payload, which is published after the detection module, which contains the machine learning algorithm for detection. The message is stored on the blockchain and can be retrieved by EV ID. Fig. 14 shows the data stored on the blockchain. Data is stored for the shown hardware prototype, with a detection module, battery, sensors, and DC programmable supply (CHROMA 5 kW, 600 V). Fig. 15 shows the analysis of the total execution time and throughput of the Hyperledger Fabric network. The performance evaluation is conducted for up to 2500 transactions using a test application interfaced with the

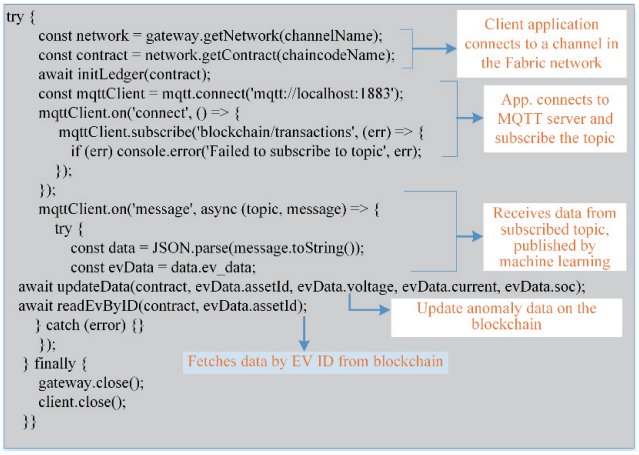


Fig. 13. The Hyperledger Fabric client application is integrated with MQTT and connects to the smart contract.

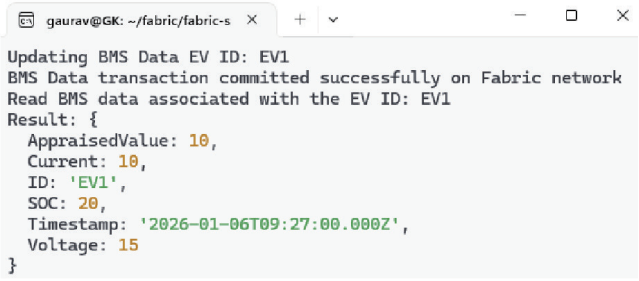


Fig. 14. Data of a single battery stored on the blockchain after the attack detection module.

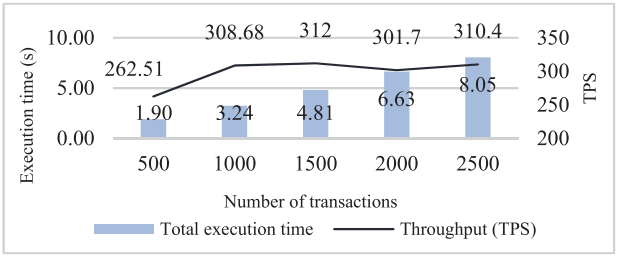


Fig. 15. Analysis of total execution time and throughput rate for the Hyperledger Fabric network.

Fabric network. The results indicate a maximum throughput of approximately 312 transactions per second (TPS). For a smaller number of transactions, the observed TPS is lower because the system waits to accumulate transactions into blocks before committing them to the ledger. Despite these advantages, the adoption of blockchain technology for IoT-based systems like BMS encounters several challenges, as outlined below:

A.Ledger Growth and Memory Constraints

As the blockchain ledger grows, maintaining the entire ledger on devices with limited memory, such as embedded systems in EVs, becomes increasingly difficult. Storing a full copy of the ledger on each node requires significant resources, and data storage within blockchain blocks can be costly in terms of both memory and processing power. In a BMS, it is crucial to decide which data should be stored on the blockchain and which can remain in off-chain databases. This balance between on-and off-chain storage is particularly important in realtime systems.

B.IoT Network-Oriented Consensus Protocol

To handle the scalability demands of a distributed BMS network with more than one IoT device, a custom consensus protocol must be developed. This protocol needs to maintain low communication complexity while ensuring high scalability across a large number of interconnected devices. Current blockchain consensus algorithms may not be efficient for the high-volume, low-latency demands of real-time BMS data. For instance, traditional proof-of-work is energy-intensive and slow, making it unsuitable for time-sensitive BMS applications.

C.Latency

Latency poses a challenge for real-time data exchange in blockchain-based BMS applications. If the blockchain server is not located nearby, it can cause delays in data validation and logging. This is particularly problematic for systems that depend on quick feedback, such as battery state estimation, charging protocols, and fault detection, where delays can impact safety and performance. Improving blockchain architecture for low-latency communication, perhaps through edge computing or local validation methods, could help address these issues.

D.Cost of Blockchain Integration

While blockchain provides security and data integrity, its operating costs remain a challenge, especially in real-time applications like BMS. The computational overhead involved in maintaining a blockchain network, particularly for consensus and data storage, can lead to high expenses related to energy, hardware, and network bandwidth. Careful evaluation of these costs against the benefits of blockchain for BMS is essential.

VI. Conclusion

This paper provided a critical review of BMS technologies. It describes the methods of CB for LIB packs. It also describes BMS communication protocols, SoC estimation methods, and the use of a private blockchain to protect BMS data. An overview of cyber-physical protocols like FlexRay shows that they can make time-sensitive tasks faster and more reliable. SoC estimation methods such as KF, SVM, and ANNs have been discussed in detail. The performance of different SoC estimation methods is computed based on RMSE and MAE. It has been observed that the ANN method provides the best prediction compared to others. Moreover, integration of AI and blockchain technology for anomaly detection and data logging is discussed. The performance of the blockchain network is 312 TPS at 1500 transactions. The Fabric network is tested up to 2500 transactions at a time.

References

[1] Y. Miao, P. Hynan, A. Von Jouanne, and A. Yokochi, "Current li-ion battery technologies in electric vehicles and opportunities for advancements," in *Energies*, vol. 12, no. 6, p. 1074, Mar. 2019.

[2] J. Yang, R. Li, K. Ma, Y. Wang, and P. Xu, "Analysis and design of cascaded DC-DC converter based battery energy storage system with distributed multimode control in data center application," in *CPSS Transactions on Power Electronics and Applications*, vol. 7, no. 3, pp. 308–318, Sept. 2022.

[3] V. M. Macharia, V. K. Garg, and D. Kumar, "A review of electric vehicle technology: Architectures, battery technology and its management system, relevant standards, application of artificial intelligence, cyber security, and interoperability challenges," in *IET Electric Power Applications*, vol. 13, no. 2, 2023.

[4] H. A. Gabbar, A. M. Othman, and M. R. Abdussami, "Review of battery management systems (BMS) development and industrial standards," in *Technologies*, vol. 9, no. 2, p. 28, Apr. 2021.

[5] N. Khan, C. A. Ooi, A. Alturki, M. Amir, Shreasth, and T. Alharbi, "A critical review of battery cell balancing techniques, optimal design, converter topologies, and performance evaluation for optimizing storage system in electric vehicles," in *Energy Reports*, vol. 11, pp. 4999–5032, Jun. 2024.

[6] S. Guguamaran and P. N. Amutha, "An efficient buck-boost converter for fast active balancing of lithium-ion battery packs in electric vehicle applications," in *Computers & Electrical Engineering*, vol. 118, p. 109429, Sept. 2024.

[7] S. Karmakar, A. K. Bohre, and T. K. Bera, "Recent advancements in cell balancing techniques of BMS for EVs: A critical review," in *IEEE Transactions on Industry Applications*, vol. 61, no. 2, pp. 3468–3484, 2025.

[8] M. S. Ramkumar et al., "Review on li-ion battery with battery management system in electrical vehicle," in *Advances in Materials Science and Engineering*, vol. 2022, pp. 1–8, May 2022.

[9] Y. Gao, C. Zhu, X. Zhang, and B. Guo, "Implementation and evaluation of a practical electrochemical-thermal model of lithium-ion batteries for EV battery management system," in *Energy*, vol. 221, p. 119688, Apr. 2021.

[10] A. Manenti, A. Abba, A. Merati, S. M. Savaresi, and A. Geraci, "A new BMS architecture based on cell redundancy," in *IEEE Transactions on Industrial Electronics*, vol. 58, no. 9, pp. 4314–4322, Sept. 2011.

[11] X. Liu, X. Xue, W. Ma, H. M. Hasanien, Z. Wei, and J. Duan, "A novel two-level equalization topology with AMPC-IVY-FLC algorithm for enhanced lithium-ion battery pack balancing," in *Energy*, vol. 335, p. 137964, Oct. 2025.

[12] Z. Chen, C. Liu, Y. Zhang, R. Yang, and G. Chen, "Hierarchical state-of-charge balancing and second-harmonic current suppressing control with a scalable DC reconfigurable battery pack," in *IEEE Transactions on Power Electronics*, vol. 39, no. 6, pp. 6758–6768, Jun. 2024.

[13] S. B S, S. Hampannavar, D. B, and B. Bairwa, "Applications of battery management system (BMS) in sustainable transportation: A comprehensive approach from battery modeling to battery integration to the power grid," in *World Electric Vehicle Journal*, vol. 13, no. 5, p. 80, May 2022.

[14] S. J. Na, J. U. Sim, B. J. Kim, D. H. Kwon, and I. H. Cho, "Design of bluetooth communication-based wireless battery management system for electric vehicles," in *IEEE Access*, vol. 12, pp. 185946–185957, 2024.

[15] H. Xu, Q. Xu, F. Duanmu, J. Shen, L. Jin, B. Gou, F. Wu, and W. Zhang, "State of charge estimation of lithium-ion batteries based on EKF integrated with PSO-LSTM for electric vehicles," in *IEEE Transactions on Transportation Electrification*, vol. 11, no. 1, pp. 2311–2321, Feb. 2025.

[16] S. Zhao, Y. Peng, Y. Zhang, and H. Wang, "Parameter estimation of power electronic converters with physics-informed machine learning," in *IEEE Transactions on Power Electronics*, vol. 37, no. 10, pp. 11567–11578, 2022.

[17] J. C. Álvarez Antón, P. J. García Nieto, C. Blanco Viejo, and J. A. Vilán Vilán, "Support vector machines used to estimate the battery state of charge," in *IEEE Transactions on Power Electronics*, vol. 28, no. 12, pp. 5919–5926, 2013.

[18] C. Chen, R. Xiong, R. Yang, W. Shen, and F. Sun, "State-of-charge estimation of lithium-ion battery using an improved neural network model and extended Kalman filter," in *Journal of Cleaner Production*, vol. 234, pp. 1153–1164, Oct. 2019.

[19] M. Ali, A. Dewan, A. K. Sahu, and M. M. Taye, "Understanding of machine learning with deep learning: Architectures, workflow, applications and future directions," in *Computers*, vol. 12, no. 5, p. 91, Apr. 2023.

[20] J. Tian, R. Xiong, W. Shen, and J. Lu, "State-of-charge estimation of $LiFePO_4$ batteries in electric vehicles: A deep-learning enabled approach," in *Applied Energy*, vol. 291, p. 116812, Jun. 2021.

[21] L. Chen, Z. Wang, Z. Lü, J. Li, B. Ji, H. Wei, and H. Pan, "A novel state-of-charge estimation method of lithium-ion batteries combining the grey model and genetic algorithms," in *IEEE Transactions on Power Electronics*, vol. 33, no. 10, pp. 8797–8807, Oct. 2018.

[22] R. Ahmed, "A comprehensive review of cloud-based lithium-ion battery management systems for electric vehicle applications," in *IEEE Access*, vol. 12, no. Aug., pp. 116259–116273, 2024.

[23] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," in *IEEE Network*, vol. 32, no. 3, pp. 78–83, May 2018.

[24] K. Kaur, G. Kaddoum, and S. Zeadally, "Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5178–5189, Aug. 2021.

[25] T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1270–1281, 2022.

[26] A. Chandwani, S. Dey, and A. Mallik, "Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and counter-measures," in *IEEE Access*, vol. 8, pp. 226982–226998, 2020.

[27] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown, and J. Lloret, "Cybersecurity risk analysis of electric vehicles charging stations," in *Sensors*, vol. 23, no. 15, p. 6716, 2023.

[28] A. Almadhor, S. Alsubai, I. Bouazzi, V. Karovic, M. Davidekova, A. A. Hejaili, and G. A. Sampedro, "Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks," in *Scientific Reports*, vol. 15, no. 1, pp. 1–20, Dec. 2025.

[29] H. Elhusseini, C. Assi, B. Moussa, R. Attallah, and A. Ghrayeb, "Blockchain, AI and S mart G rids: The three musketeers to a decentralized EV charging infrastructure," in *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 24–29, Jun. 2020.

[30] Data Security Council of India (DSCI), Seqrite, and V. Godse, "India Cyber Threat Report 2025," 2025. [Online]. Available: https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf

[31] V. Chamola, A. Sancheti, S. Chakravarty, N. Kumar, and M. Guizani, "An IoT and edge computing based framework for charge scheduling and EV selection in V2G systems," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 10569–10580, Oct. 2020.

[32] A. Samanta and S. S. Williamson, "A survey of wireless battery management system: Topology, emerging trends, and challenges," in *Electronics*, vol. 10, no. 18, pp. 1–12, 2021.

[33] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun, and Y. Zhang, "A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly," in *High-Confidence Computers*, vol. 4, no. 2, p. 100211, Jun. 2024.

[34] S. Mishra, S. Verma, S. Chowdhury, A. Gaur, S. Mohapatra, G. Dwivedi, and P. Verma, "A comprehensive review on developments in electric vehicle charging station infrastructure and present scenario of India," in *Sustainability*, vol. 13, no. 4, pp. 1–20, Feb. 2021.

[35] K. Sevdari, P. B. Andersen, and M. Marinelli, "Aggregation and control of electric vehicles AC charging for grid services delivery," in *IEEE Transactions on Smart Grid*, vol. PP, no. 9, p. 1, 2024.

[36] S. S. G. Acharige, M. E. Haque, M. T. Arif, N. Hosseinzadeh, K. N. Hasan, and A. M. T. Oo, "Review of electric vehicle charging technologies, standards, architectures, and converter configurations," in *IEEE Access*, vol. 11, pp. 41218–41255, Feb. 2023.

[37] M. S. Mastoi, S. Zhuang, H. M. Munir, M. Hassan, M. Usman, S. S. H. Bukhari, and J. S. Ro, "An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends," in *Energy Reports*, vol. 8, pp. 11504–11529, 2022.

[38] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," in *IEEE Transactions on Industrial Electronics*, vol. 68, no. 1, pp. 478–487, Jan. 2021.

[39] V. S. Rao, G. S. Sajja, V. B. Manur, S. Arandhakar, and V. B. M. Krishna, "An exploratory study on intelligent active cell balancing of electric vehicle battery management and performance using machine learning algorithms," in *Results in Engineering*, vol. 25, p. 104524, Mar. 2025.

[40] Shreasth, C. A. Ooi, N. Khan, M. K. B. M. Desa, M. K. Ishak, and K. Ammar, "A novel active lithium-ion cell balancing method based on charging and discharging state of power in electric vehicles," in *Scientific Reports*, vol. 15, no. 1, pp. 1–25, Dec. 2025.

[41] N. Khan, C. A. Oos, Shreasth, A. Alturki, M. K. M. Desa, M. Amir, A. B. Ahmad, and M. K. Ishak, "A novel active cell balancing topology for serially connected Li-ion cells in the battery pack for electric vehicle applications," in *Scientific Reports*, vol. 14, no. 1, pp. 1–21, Dec. 2024.

[42] M. Y. Kim, C. H. Kim, J. H. Kim, and G. W. Moon, "A chain structure of switched capacitor for improved cell balancing speed of lithium-ion batteries," in *IEEE Transactions on Industrial Electronics*, vol. 61, no. 8, pp. 3989–3999, Aug. 2014.

[43] Y. Ye, J. Lin, Z. Li, and X. Wang, "Double-tiered cell balancing system with switched-capacitor and switched-inductor," in *IEEE Access*, vol. 7, pp. 183356–183364, 2019.

[44] K. M. Lee, S. W. Lee, Y. G. Choi, and B. Kang, "Active balancing of li-ion battery cells using transformer as energy carrier," in *IEEE Transactions on Industrial Electronics*, vol. 64, no. 2, pp. 1251–1257, Feb. 2017.

[45] V. B. Vulligaddala, S. Vernekar, S. Singamla, R. K. Adusumalli, and V. Ele, "A 7-cell, stackable, li-ion monitoring and active/passive balancing IC with in-built cell balancing switches for electric and hybrid vehicles," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3335–3344, May 2020.

[46] Z. B. Omariba, L. Zhang, and D. Sun, "Review of battery cell balancing methodologies for optimizing battery pack performance in electric vehicles," in *IEEE Access*, vol. 7, pp. 129335–129352, 2019.

[47] D. Thiruvonasundari and K. Deepa, "Optimized passive cell balancing for fast charging in electric vehicle," in *IETE Journal of Research*, vol. 69, no. 4, pp. 2089–2097, May 2023.

[48] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," in *Computer Science Review*, vol. 13–14, pp. 1–38, Aug. 2014.

[49] R. Zurawski and M. C. Zhou, "Petri nets and industrialapplications: A tutorial," in *IEEE Transactions on Industrial Electronics*, vol. 41, no. 6, pp. 567–583, 1994.

[50] H. Wu and W. Wang, "A game theory based collaborative security detection method for internet of things systems," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1432–1445, Jun. 2018.

[51] J. Ye , L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber-physical security of power train systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," in *IEEE Journal of Emerging and Selected Topics in Power Electronic*s, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[52] F. Hosseinabadi, S. Chakraborty, S. K. Bhoi, G. Prochart, D. Hrvanovic, and O. Hegazy, "A comprehensive overview of reliability assessment strategies and testing of oower electronics converters," in *IEEE Open Journal of Industry Applications*, vol. 5, no. January, pp. 473–512, 2024.

[53] S. Murlidharan, V. Ravulakole, J. Karnati, and H. Malik, "Battery management system: threat modeling, vulnerablity analysis, and cybersecurity stategy," in *IEEE Access*, vol. 13, pp. 37198–37220, 2025.

[54] B. Cyr, J. Mahmod, and U. Guin, "Low-cost and secure firmware obfuscation method for protecting electronic systems from cloning," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3700–3711, Apr. 2019.

[55] D. Ronanki and H. Karneddi, "Electric vehicle charging infrastructure: Review, cyber security considerations, potential impacts, counter-measures, and future trends," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 12, no. 1, pp. 242–256, Feb. 2024.

[56] M. Moraitis, "FPGA bitstream modification: Attacks and counter-measures," in *IEEE Access*, vol. 11, pp. 127931–127955, 2023.

[57] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting," in *Scientific Reports*, vol. 14, no. 1, p. 8169, Apr. 2024.

[58] B. V. P. Prasad, J. J. Tang, and S. J. Luo, "Design and implementation of SAE J1939 vehicle diagnostics system," in *Proceedings of 2019 IEEE International Conference on Computation, Communication and Engineering (ICCCE)*, Fujian, China, 2019, pp. 71–74.

[59] A. Singhal, "Web Services Security: Challenges and Techniques," in *Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)*, Bologna, Italy, 2007, pp. 282–282.

[60] J. Yi, H. An, Y. Xing, J. Li, G. Zhang, O. Bamisile, K. Yang, and Y. Xu, "A cyber attack detection strategy for plug-in electric vehicles during charging based on CEEMDAN and broad learning system," in *Energy Reports*, vol. 9, pp. 80–88, May 2023.

[61] H. Cui, X. Dong, H. Deng, M. Dehghani, K. Alsubhi, and H. M. A. Aljahdali, "Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on hilbert-huang transform and deep learning," in *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15885–15894, Jul. 2021.

[62] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," in *IEEE Transactions on Transportation Electrification*, vol. 7, no. 3, pp. 2010–2022, Sept. 2021.

[63] A. Hafeez, H. Malik, O. Avatefipour, P. R. Rongali, and S. Zehra, "Comparative study of CAN-bus and FlexRay protocols for in-vehicle communication," in *Proceedings of SAE World Congress Experience WCX™ 17*, Michigan, pp. 46–53, 2017.

[64] K. Wang, D. Peng, L. Song, and H. Zhang, "Implementation of Modbus communication protocol based on ARM Coretx-M0," in *Proceedings of 2014 IEEE International Conference on System Science and Engineering (ICSSE)*, Shanghai, 2014, pp. 69–73.

[65] K. E. Jeon, J. She, P. Soonsawad and P. C. Ng, "BLE beacons for internet of things applications: Survey, challenges, and opportunities," in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 811–828, Apr. 2018.

[66] R. Shaw and B. Jackman, "An introduction to FlexRay as an industrial network," in *Proceedings of 2008 IEEE International Symposium on Industrial Electronics*, Cambridge, UK, 2008, pp. 1849–1854.

[67] Y. Chen, R. Li, Z. Sun, L. Zhao, and X. Guo, "SOC estimation of retired lithium-ion batteries for electric vehicle with improved particle filter by H-infinity filter," in *Energy Reports*, vol. 9, pp. 1937–1947, Dec. 2023.

[68] B. Xia, Z. Zheng, Z. Lao, W. Wang, S. Wei, Y. Lai, and M. Wang, "Strong tracking of a H-infinity filter in lithium-ion battery state of charge estimation," in *Energies*, vol. 11, no. 6, p. 1481, Jun. 2018.

[69] J. Meng, M. Ricco, G. Luo, M. Swierczynski, D. Stroe, A. Stroe, and R. Teodorescu, "An overview and comparison of online implementable SOC estimation methods for Lithium-ion battery," in *IEEE Transactions on Industry Applications*, vol. 54, no. 2, pp. 1583–1591, Mar.-Apr. 2018.

[70] F. Zheng, Y. Xing, J. Jiang, B. Sun, J. Kim, and M. Pecht, "Influence of different open circuit voltage tests on state of charge online estimation for lithium-ion batteries," in *Applied Energy*, vol. 183, pp. 513–525, Dec. 2016.

[71] X. Zhang, X. Li, K. Yang, and Z. Wang, "Lithium-ion battery modeling and state of charge prediction based on fractional-order calculus," in *Mathematics*, vol. 11, no. 15, 2023.

[72] E. Buchicchio, A. De Angelis, F. Santoni, P. Carbone, F. Bianconi, and F. Smeraldi, "Battery SOC estimation from EIS data based on machine learning and equivalent circuit model," in *Energy*, vol. 283, p. 128461, Nov. 2023.

[73] H. Qu, H. Kuang, Q. Wang, J. Li, and L. You, "A physics-informed and attention-based graph learning approach for regional electric vehicle charging demand prediction," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 10, pp. 14284–14297, Oct. 2024.

[74] H. B. Sassi, F. Errahimi, N. Es-Sbai, and C. Alaoui, "Comparative study of ANN/KF for on-board SOC estimation for vehicular applications," in *Journal of Energy Storage*, vol. 25, p. 100822, Oct. 2019.

[75] C. Mehta, A. V. Sant, and P. Sharma, "Optimized ANN for LiFePO4 battery charge estimation using principal components based feature generation," in *Green Energy and Intelligent Transportation*, vol. 3, no. 4, p. 100175, Aug. 2024.

[76] A. A. Hussein, "Capacity fade estimation in electric vehicle Li-ion batteries using artificial neural networks," in *IEEE Transactions on Industry Applications*, vol. 51, no. 3, pp. 2321–2330, May 2015.

[77] J. Misra and I. Saha, "Artificial neural networks in hardware: A survey of two decades of progress," in *Neurocomputing*, vol. 74, no. 1–3, pp. 239–255, Dec. 2010.

[78] S. Park, S. Moura, and K. Lee, "Integration of hardware and software for battery hardware-in-the-loop toward battery artificial intelligence," in *IEEE Transactions on Transportation Electrification*, vol. 10, no. 1, pp. 888–900, Mar. 2024.

[79] M. Risso, A. Burrello, and D. J. Pagliari, "Optimizing DNN inference on multi-accelerator SoCs at training-time," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 44, no. 9, pp. 3532–3545, Sept. 2025.

[80] Y. Xing, W. He, M. Pecht, and K. L. Tsui, "State of charge estimation of lithium-ion batteries using the open-circuit voltage at various ambient temperatures," in *Applied Energy*, vol. 113, pp. 106–115, Jan. 2014.

[81] N. Shateri, Z. Shi, D. J. Auger, and A. Fotouhi, "Lithium-sulfur cell state of charge estimation using a classification technique," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 212–224, Jan. 2021.

[82] D. N. T. How, M. A. Hannan, M. S. H. Lipu, K. S. M. Sahari, P. J. Ker, and K. M. Muttaqi, "State-of-charge estimation of li-ion battery in electric vehicles: A deep neural network approach," in *IEEE Transactions on Industry Applications*, vol. 56, no. 5, pp. 5565–5574, Sept. 2020.

[83] D. Paizulamu, L. Cheng, H. Xu, Y. Zhuang, N. Qi, and S. Ci, "$LiFePO_4$ battery SOC estimation under OCV–SOC curve error based on adaptive multimodel Kalman filter," in *IEEE Transactions on Transportation Electrification*, vol. 11, no. 4, pp. 8833–8846, Aug. 2025.

[84] P. Shrivastava, T. K. Soon, M. Y. I. Bin Idris, and S. Mekhilef, "Overview of model-based online state-of-charge estimation using Kalman filter family for lithium-ion batteries," in *Renewable and Sustainable Energy Reviews*, vol. 113, p. 109233, Oct. 2019.

Gaurav Kumar is a Ph.D. student in the Electrical and Electronics Engineering Department of the National Institute of Technology, Goa. He has done M.Tech. degree in power electronics and power systems from the National Institute of Technology, Goa, India, in 2017. His research interests include electric vehicles, renewable energy, and DC-DC converters. He has achieved the MHRD scholarship during his M.Tech. degree.

Suresh Mikkili received the B.Tech. degree in electrical and electronics engineering (EEE) from S.I.T.E, T.P. Gudem, India, in 2006. He received the M.Tech. and the Ph.D. degrees in electrical engineering from the National Institute of Technology, Rourkela, India, in 2008 and 2013, respectively. He is currently working as an Assistant Professor in the department of EEE at National Institute of Technology Goa (NIT Goa), India. He has been Head of the EEE department at NIT goa from June 2014 to November 2015. Since, September 2015, he is the Dean, Student welfare at NIT Goa. His research interests include power quality improvement issues, active filters, power electronics applications to power systems, applications of soft computing techniques and renewable energy sources. He has authored a book entitled *Power Quality Issues: Current Harmonics*, published in CRC Press, Taylor & Francis Group, August 2015, ISBN 9781498729628. He has reported results of his research (160+ articles) in reputed international journals (SCI/SCI-E) and conferences (annual/biannual/biennial).