Cybersecurity of Battery Management System

Subjects: Engineering, Electrical & Electronic

Contributor: Farshid Naseri , Zahra Kazemi , Peter Gorm Larsen , Mohammad Mehdi Arefi , Erik Schaltz

Battery management systems (BMSs) are critical to ensure the efficiency and safety of high-power battery energy storage systems (BESSs) in vehicular and stationary applications. The proliferation of battery big data and cloud computing advancements has led to the development of a new generation of BMSs, named Cloud BMS (CBMS), aiming to improve the performance and safety of BESSs. The CBMS is a cyber-physical system with connectivity between the physical BMS and a cloud-based virtual BMS, which is realized through a communication channel such as Internet of Things. Compared to the traditional BMS, the CBMS offers significantly higher computational resources, leveraging the implementation of advanced digital twin models and best-in-class algorithms in the BMS software, which will provide superior performances.

electric vehicle | battery management systems | cloud computing | cybersecurity | cyberattacks | blockchain | cyber-physical systems | Internet of Things

1. Battery Energy Storage System Cybersecurity

The operation of bidirectional electric vehicle supply equipment (EVSEs) with Vehicle-to-Grid (V2G) capability (also referred to as smart charging equipment [1]) should usually be scheduled and coordinated through effective communication channels between different stakeholders, including the electric vehicle (EV) owners, charge station operators, and grid operators [2]. V2G offers several advantages through different ancillary services such as peak shaving, demand side management, voltage/frequency stability support, reactive power compensation [1], etc. However, V2G has some challenging security issues [1]. The sum effect of charge stations can have great impacts on the grid, and cyberattacks against them can endanger the operation and stability of the grid. Compared to low-power EVSEs, the cyberattack impacts on the grid are more important in the case of high-power fast-charging EVSEs [3]. Several studies have thus analyzed the cybersecurity of charging stations [4][5]. The authors of [2] analyzed the impact of the false data injection (FDI) attack falsifying the charge station power request, which resulted in a violation of the peak power constraint and accordingly caused financial penalties and triggered technical problems in the upstream grid [2]. In [6], the cybersecurity of wireless power transfer modules (WPTMs) for EV fast charging was discussed. Cyberattacks against charging station controllers were analyzed and it was accordingly concluded that the attacks can disrupt the operation or cause failures in the physical chargers such as the occurrence of short-circuits. In [4], the vulnerability of the CHAdeMO charge protocol which also has bidirectional energy transfer capability was highlighted. Despite ensuring safety, CHAdeMO does not offer secure communications, which means the messages are not encrypted when the charger is connected to the CAN bus and BMS. The cybersecurity of EVSEs was also explored in [7][8], which discovered some cybersecurity

vulnerabilities of EVSEs, e.g., vulnerability of combined charging system (CCS) charge protocol to electromagnetic side-channel attacks. Nevertheless, CCS has generally higher security compared to CHAdeMO, e.g., it requires the specification of digital certificates to authenticate different devices or transport layer security (TLS)-based encryption, as per ISO 15118 [9]. With CCS, automated authentication and authorization can also be fulfilled through plug and charge (PnC) services [4]. A comparison of different charging protocols and their security features was presented in [4]. The impact of integrity attacks on the power electronics components of EV onboard chargers (OBCs) was examined in [10]. As discussed, such attacks can undesirably influence the FPGA controllers of the OBCs, establish fake messages from OBC to other vehicle ECUs listening to the CAN bus, and interfere with the functionalities of the BMS. Potential attack points can be interfaces of the CAN bus for BMS and OBCs, interfaces of EVSE, V2G interfaces, and IoT interfaces with the vehicle and CBMS [10].

The cybersecurity of large-scale stationary BESSs for grid applications such as voltage/frequency regulation, black start, etc., has partly been discussed in the literature [11]. In [12], published by Sandia National Laboratories, detailed discussions related to the physical security and cybersecurity of stationary BESSs were provided, where it was argued that security should be considered as a design factor in the battery and BMS early development cycles (otherwise it becomes a costly and less effective solution to add at later stages). Some studies have also been fulfilled on other aspects of vehicle cybersecurity, such as cybersecurity in autonomous cars [13].

In the following, the classification of different attack types/scenarios, potential impacts, and possible countermeasures are presented and discussed.

2. Attack Types and Scenarios

The CBMS is a CPS, and IoT plays the main role in connecting the physical and virtual parts. Thus, many of the IoT security threats and requirements can be applied to CBMSs as well [14][15]. Based on the cybersecurity literature, a secure CPS must satisfy three main requirements, related to confidentiality, integrity, and availability, also known as CIA [16]. The same CIA security requirements can be applied to the CBMS, as summarized in **Figure 1**.

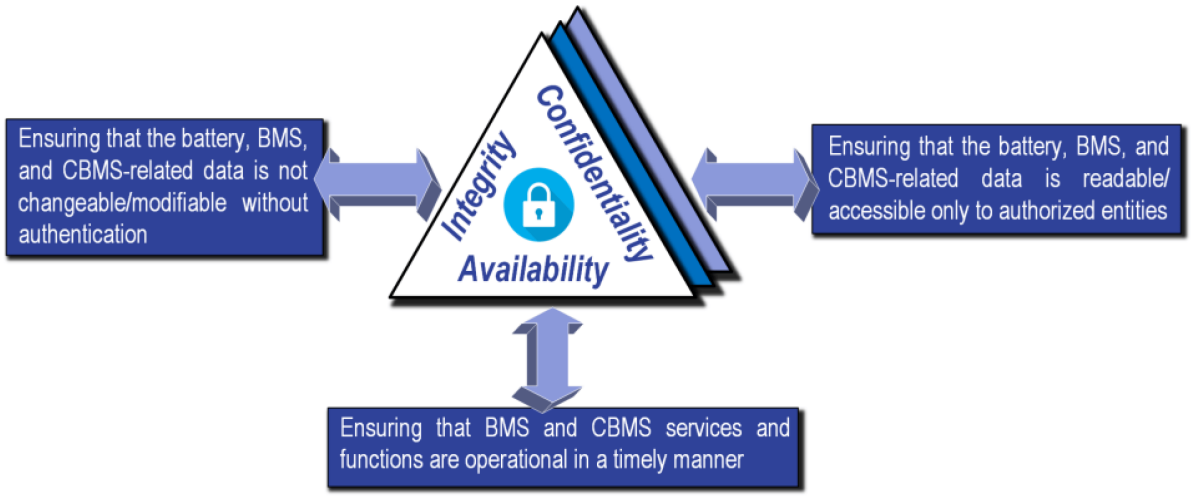

Figure 1. CIA requirements for CBMS cybersecurity.

As explained in the figure, the CIA requirements ensure that the battery and CBMS data cannot be accessed, changed/modified, disrupted, or interrupted without proper authentication. The concurrent assurance of the CIA requirements can result in an acceptably secure CBMS. Different types and scenarios of attacks can be potentially launched to violate the CIA's conditions. The attack categorization and definitions can be slightly different for different application contexts. **Figure 2** depicts the CBMS cyberattacks classification depending on the CIA requirements attacked [11][17][18]. It should be noted that in some attack conditions, more than one CIA requirement might become compromised.

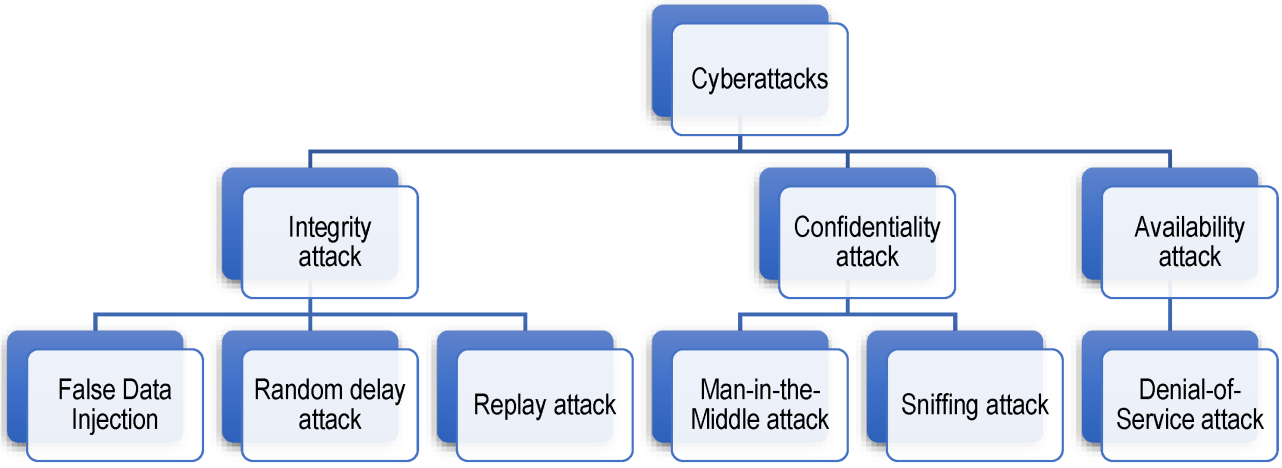

Figure 2. Classification of different potential cyberattacks against CBMS.

The CBMS attack scenarios are further explained as follows.

- Confidentiality attacks: The confidentiality attack refers to unauthorized access to the battery/BMS data without directly targeting to damage the system [11]. There are two types of confidentiality attacks: (1) sniffing attack (also known as snooping attack), in which the attacker only can passively listen to the data traffic (in-vehicle through CAN bus or extra-vehicle through IoT communication), and (2) man-in-the-middle (MitM) attack, in which the attacker might also have the possibility to affect the data flow, e.g., via eavesdropping, in which the attacker can relay data between two communication nodes. Regarding sniffing attacks, Ref. [17] illustrates bandwidth sniffing attacks in which the attacker can gain bandwidth information used between the BMS and CBMS to discover some information about BMS, e.g., active components of the BMS and their related activities. The graphical description of the bandwidth sniffing attack is shown in **Figure 3**. This attack is considered an indirect side-channel attack in which indirect information is used to gain knowledge about the system, with the possible intention to construct and launch more complex attack scenarios [17]. In **Figure 3**, activities refer to BMS functions or processes.

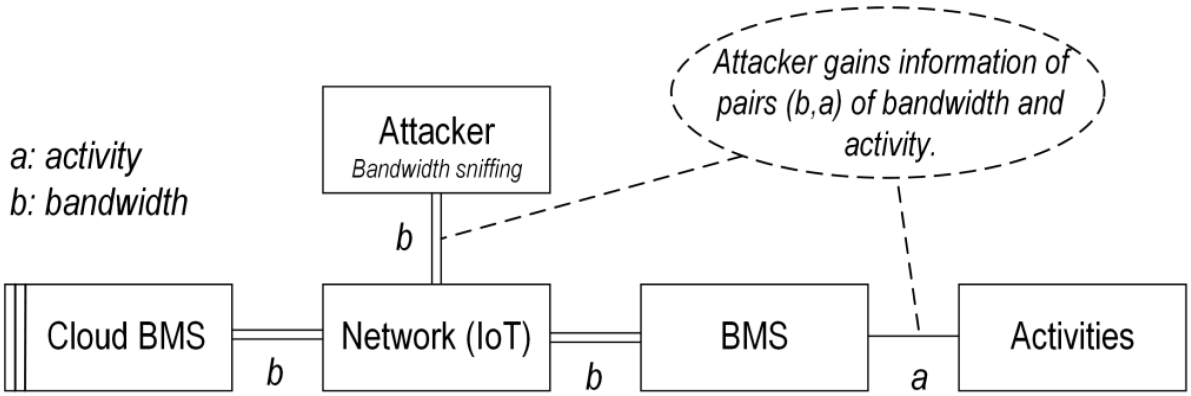

Figure 3. Illustration of the bandwidth sniffing attack.

Confidentiality attacks are generally the least dangerous attack type since they can be mostly launched in a passive format and cannot directly compromise functional safety. Nevertheless, the information/data stolen from the CBMS database (storage attack) can be used to design more complicated attack scenarios such as FDI attacks. Confidentiality can be compromised via physical and/or network attacks. The latter can be fulfilled through direct download, spyware/malware, etc. Brute-forcing and cloning may also be considered subcategories of confidentiality attacks. These attacks aim to bypass authentication processes through the hack of passcodes or security tags to access the CBMS servers or the IoT.

- Integrity attacks: These refer to malicious cyberincidents that lead to the corruption, unauthorized modification, or alteration of the CBMS algorithms/data [4]. Three types of integrity attacks may be considered within the CBMS context: (1) FDI attack refers to deliberate manipulation of the CBMS data such as VIT measurements of cells by injecting false data vectors into the original data. The FDI attacks have a complicated nature and their construction requires some knowledge about the behavior and model of the BESS such that they would normally bypass or circumvent bad data detectors. (2) Random delay attacks are where a random delay will be deliberately introduced to the sequence of BMS control commands or data. (3) Replay attacks occur by wiretapping and repeatedly broadcasting the battery/CBMS measurements/data. Integrity attacks have great potential to compromise EV/pack safety, e.g., to falsify the SoX estimation results, delay the performance of actuators in the battery pack, etc. The graphic illustration of the FDI attack is shown in **Figure 4**a. Ref [17] presents two different versions of the FDI attack: (1) Injecting control commands to take control of the battery pack; (2) injecting falsified data to deceive the BMS as if the data are originally provided by CBMS, causing troubles for BMS algorithms such as SoX estimation. The two FDI versions are illustrated in **Figure 4**b,c [17].

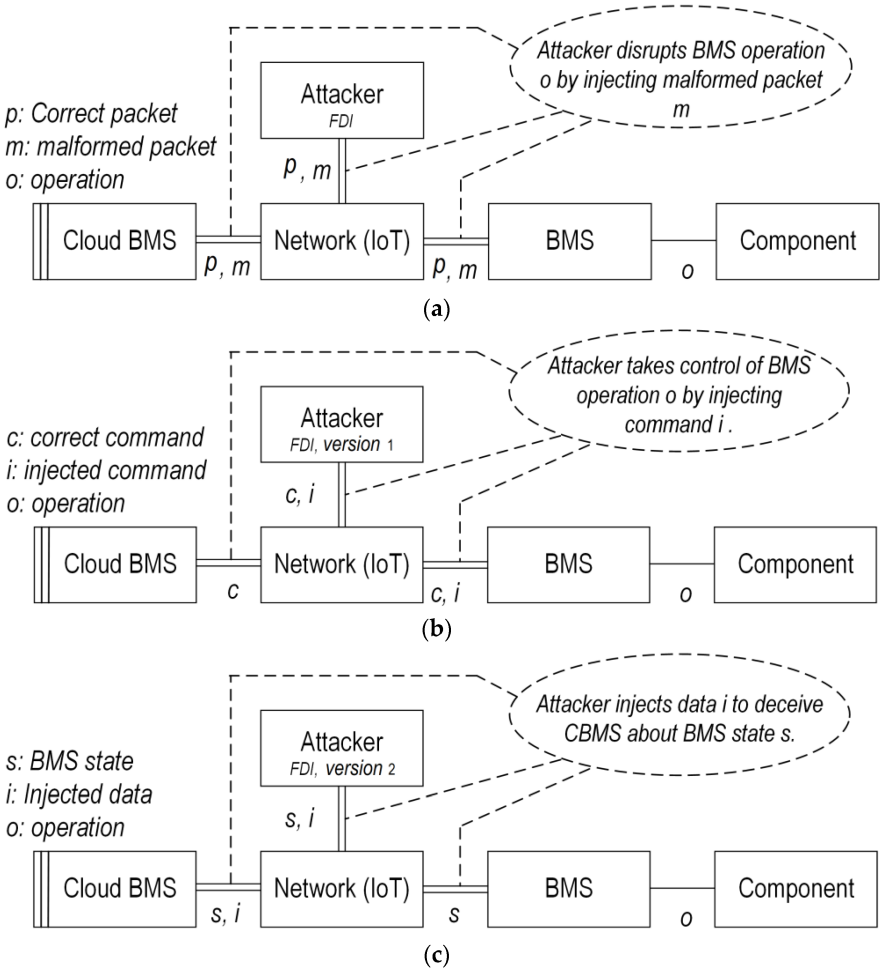

Figure 4. (**a**) Concept illustration of the FDI attack. (**b**) Variant 1 of the FDI attack. (**c**) Variant 2 of the FDI attack.

Likewise, **Figure 5** shows the block diagram of the delay attack in which the attacker aims to inject a delay in the transmission of data packets in the communication links.

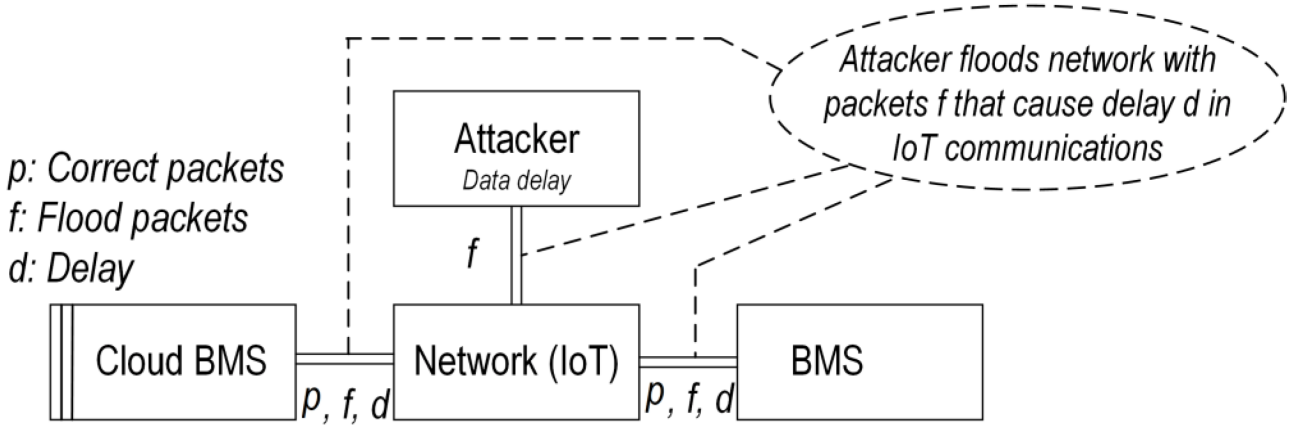

Figure 5. Illustration of the data delay attack.

- Availability attacks: Refers to the denial-of-service (DoS), in which the attacker seeks to make the CBMS services unavailable to EVs [19]. DoS can be fulfilled by either flooding the network or crashing the network.

Flooding happens when the IoT receives too much information to buffer, which will slow down and eventually stop its services. The most challenging DoS is the distributed DoS (DDoS), in which multiple attackers orchestrate a synchronized DoS attack on CBMS.

In practice, loosely-secured CBMS-IoT networks are vulnerable to all types of attacks described before [4]. For instance, if the attacker succeeds to create fake routers or unauthorized IoT nodes, it can potentially make spoofed, altered, or replayed routing information in the network layer protocol. Likewise, sending malicious data packets might result in packet collision and data loss. For some protocols, such as MQTT, the entire IoT network will be compromised if the attacker manages to access the broker [4]. In [18], different cyberattack possibilities on the stationary BESSs were analyzed. For instance, a random delay attack in which a constant high SOC is introduced to the system was analyzed, where the attack objective was to overdischarge the battery to accelerate the battery degradation.

Malware injection through EVSEs was discussed in [1]. EVSEs are placed in public without any physical access restrictions. The lack of physical security protocols poses the risk of the injection of malware that can steal sensitive data such as battery/EV data, personal information, payment information, etc. One compromised EVSE opens doors to a variety of exploitable vulnerabilities [3]. For instance, the polluted EVSEs pose a risk to BMS since the malware can be passed to BMS or other vehicle ECUs through the CAN interface [1]. The attack surface can be exponentially scaled if malware infection passes to the CBMS that is shared among an EV fleet. For example, if CBMS algorithms are trained and/or operated based on EV fleet data rather than individual EVs, the attack on one EV can impact the performance of other EVs batteries. While this is the worst-case scenario, the exact attack conditions and impacts will depend on the implementation strategy of the CBMS and the communication nodes that will be compromised by attackers.

A potential type of attack that threatens BMSs with wireless communication is the EMI attack. External malicious EMI sources can disrupt the performance of wireless communication links, e.g., in long vehicles such as electric buses where the long physical distance between the slave boards and master PMU weakens the data transmission. A malicious EMI source onboard a bus can potentially disrupt the BMS performance in such conditions. The EMI attack has not been explored in the BMS literature before. EMI attacks are discussed as potential future research.

Regarding the attack paths, communication nodes inside and outside EVs can be potential attack points. This includes in-vehicle ports/connections such as CAN or LIN bus interfaces (internal gateways), OBD-II, SD slot, USB interfaces, etc., or extra-vehicle connections based on Bluetooth, WLAN, IoT gateway MQTT protocol, Modbus TCP/IP [20][21], CBMS interfaces to the cloud, etc. [22]. CAN communication or its variations such as CAN 2.0B and CAN-FD (CAN bus with flexible data rate) are the prevailing protocol adopted in the automotive sector for communication between the vehicle ECUs. Due to its robustness and cost-effectiveness, it is usually used for data transmission related to safety-critical systems including BMS, anti-lock braking systems (ABSs), steering systems, etc. Lower important information such as data related to door locks, rain sensors, entertainment, navigation, etc., is generally transmitted using LIN, FlewRay, or MOST protocols [22]. Despite its robustness, CAN protocols do not have adequate authentication or data encryption mechanisms. The CAN bus access points through the IoT

gateway, OBD-II port, etc., are thus potential attack points where malicious attackers can grasp battery and BMS-related data, replay or change the data, etc., to interrupt the performance of the battery pack and EV. A tree diagram of possible attack paths is presented in [23], which covers vulnerabilities at three different layers, namely, the communication layer through alteration of data packets in the communication channel, the control layer through interruption of the control computations, and the sensing layer through compromising sensor/meter readings. In [24], evaluation metrics are established to assess the impact of cyberattacks on the ECU of connected or automated EVs. Communications related to V2X IoT, Global Positioning System (GPS) data, wheel sensors, etc., are considered potential attack spots. Likewise, the model predictive control of EV driving speed and torque was considered as the case study, but it is argued that the same metrics can be applied to other EV ECUs, including the CBMS. The analysis was used to identify the potential weak links in the control system design. In a broader sense, Ref. [25] highlights cyberattacks during BESS manufacturing processes and discusses that such attacks can affect the performance of CBMS and its algorithms that rely on production data, e.g., ML-based techniques.

3. Cyber-Risks and Impacts

Assessment of the cybersecurity risk is challenging and depends on different factors including the use case, implementation mechanisms and strategies, type of interaction between BMS and CBMS, etc. The severity of the damage to the battery may also differ depending on the condition of the battery when it was attacked, e.g., at high SoC values, more severe damage can happen [25]. The impacts can generally be classified as follows:

- *Functional impacts*: These occur when a system, component, function, or algorithm in CBMS is no longer functioning correctly due to a malicious cyberattack. For instance, [26] refers to a “denial-of-charging” cyberattack that falsifies the SoC estimation algorithm in BMS to prevent the battery pack from being fully charged. This could lead to prolonged driving due to the lower charge available. Integrity attacks can lead to malfunctioning of BMS algorithms, e.g., causing divergence of SoX estimators, resulting in suboptimal solutions in thermal and energy management, etc.

- *Financial and privacy losses*: Attacks against BMS sensors or algorithms such as voltage sensors or SoC/SoP estimation algorithms can result in BMS malfunctioning, which in turn can result in accelerated degradation of the battery [27]. For example, falsified SoC data can cause the battery to be operated at very high or very low SoC regions, which will speed up the aging processes of the battery. Falsified SoH data can result in wrong battery maintenance implications, e.g., the battery could either be serviced/maintained too soon when maintenance is not required or too late when the battery has undergone expensive damages. Manipulation of the cooling-related sensors and/or algorithms may result in accelerated aging of the battery. In one case example, the BMS was compromised to turn on the battery heater, draining all the charge [28]. Such scenarios can occur, for example, through false injecting of CAN messages to the EV CAN bus (e.g., through CHAdeMO charger connection). Likewise, critical information can be compromised under cyberattacks, which could lead to loss of privacy, e.g., GPS data, driving profiles, etc. Last, but not least, technology and intellectual property theft can occur by stealing confidential manufacturing data (battery cell data, BMS design data, layouts, etc.) through confidentiality attacks.

- *Safety impacts*: BMS is usually programmed with hard limits to avoid safety risks, e.g., by comparing cell voltages to the safe voltage limits. However, such limits might be overridden under malicious BMS firmware updates, which may result in battery overcharge and/or overdischarge. Small overcharge will result in accelerated aging of the battery, while overcharge in the scale of minutes might cause more serious risks such as internal short-circuits and thermal runaways [27]. Cooling system performance may also be interpreted through cyberattacks against thermal management systems, leading to the thermal runaway risk. Thus, it is important to devise efficient failsafes (e.g., mechanical override design features) to disconnect the battery in such cases [29]. Poor estimation of SoX data might also result in conditions that compromise the safety, e.g., leading to lower maneuverability of the EV on the road or misleading drivers about the achievable EV performance such as acceleration, etc. There is also a safety risk when the battery pack is disconnected, or its performance is limited due to a cyberattack while the EV is in driving mode.

- *Side impacts*: The CBMS large databases can be used to develop battery models and algorithms for other lifecycle stages such as second-life battery applications. Attacks against the CBMS database can result in data poisoning and data corruption and this will further affect the battery and BMS designs that are fulfilled based on these corrupted datasets.

As discussed in [27], the impacts of cyberattacks can also be classified as having a temporary effect (such as draining battery charge, which would temporarily reduce the achievable driving range) or permanent damage (such as reduced battery age). When EVs have interactions with the grid (e.g., through V2G and G2V), attacks on CBMS can cause trouble for the power grid as well. These aspects have been examined in several works. For example, malicious firmware updates can disable EV chargers, which can potentially interrupt emergency and medical services, manufacturing, defense, etc. [30]. Falsified BMS data such as wrong SoC and charge/power demand data can corrupt the performance of the power system, leading to overfrequency [31], underfrequency [32], voltage deviations [32][33], etc. [33]. In a recent study [34], MitM cyberattacks on grid BESSs were emulated, which proved a variety of impacts: prosumer financial losses, including a +36% increase in the electricity bill and a +46% increase in the peak power consumption, which in turn will affect the grid performance.

4. Cloud Battery Management System Attack Detection Methods and Mitigation Strategies

No CPS can be considered 100% secured when they have data flow to/from them, and despite the fact that previously discussed measures can reduce the cyberattack probability, the BMS still might be compromised. Nevertheless, when an attack is successfully launched, the system should be able to detect and take proper action to reduce the risk. In safety-critical situations, the BMS should shut off the battery pack operation, e.g., to avoid a thermal runaway. Some methods have considered nonbinary decisions, for example, slowly backing off the current in some stages [35], giving a warning to the operator instead of shutting off the battery pack [36], or extending the time before shutting down the battery. To take timely action, it is critical to devise effective attack detection mechanisms. The literature regarding CBMS cyberattack detection is rare. A basic approach to detect attacks is based on intrusion detection systems (IDSs). An IDS monitors the network traffic and checks it for any sign of

intrusion or malicious activities [37]. For example, it can compare the network traffic against a database of known network patterns under cyberattacks and can send an alarm if a match is found [37]. Another approach for cyberattack detection is referred to as behavior-based detection [38]. In this approach, the behavior of a network, system, data, or signal will be compared to a baseline describing nonattack conditions. The residual signals describing the differences between the behavior of the actual index and the baseline index show a potential cyberattack. In this regard, one effective solution is to apply ML techniques to analyze large volumes of BMS data and to identify patterns of attacked and nonattacked conditions and distinguish between them [38]. An example of ML-based attack detection is presented in [39], in which an ML-based trust framework for battery sensory data was proposed. The framework is based on false sensor data detection (FSDD) which enables detection of undependable battery data using deep learning algorithms. Likewise, Ref. [40] presented algorithms for the detection of denial-of-charging and overcharging attacks. Two static and observer-based dynamic cyberattack detectors were designed. The static detector is based on the measurements while the dynamic detector utilizes both battery measurements and models to detect the attacks, and it was shown that the latter achieves superior attack detectability performance [40]. A more detailed review of cyberattack detection techniques can be found in [41][42][43].

5. Methods for Enhancing the Cybersecurity of the Battery Management System/Cloud Battery Management System

Security plays a critical role in EV's functional safety. Different security measures related to hardware security, software update security, penetration test, and code reviews are usually applied in the automotive industry. This includes approaches based on information encryption and authentication or using firewalls for communication between vehicle devices and external networks [24]. The CBMS should similarly emplace appropriate protection measures at both software and hardware levels to protect it against any unauthorized alteration. According to the literature, several measures can be taken into account to enhance the cybersecurity of the CBMS. As outlined in [11], these measures can be applied in three different steps: (1) architecture design step (e.g., considering a distributed or decentralized CBMS instead of centralized implementation to enhance security), (2) communication system design step (e.g., considering security protocols, data encryption, user authentication, etc.), and (3) top-up protection (e.g., by protecting BMS sensors, etc.). The protection measures are described in the following:

- *Blockchain technology*: Blockchain is a secure distributed database for maintaining constantly growing data records. It was initially developed to secure cryptocurrency transactions, but lately, it has been explored for new cloud applications including CBMSs. Concerning the CBMSs, it has been discussed that the blockchain can be used to enhance both software and hardware aspects [39]. For instance, the blockchain can be used to manage critical activities related to the transaction and sharing of battery data between the CBMS and the BMS terminal nodes [19]. The blockchain transactions are time-stamped, cryptic, and immutable, meaning that the data cannot be read or modified from single communication nodes. Furthermore, transactions will be endorsed by corresponding nodes so the authenticity of the communication nodes and data can be validated. Likewise, the distributed/decentralized nature of the blockchain significantly lowers the cybersecurity risk in case of

successful attacks on one or more communication nodes. Key features of blockchain technology are described in **Figure 6** [44].

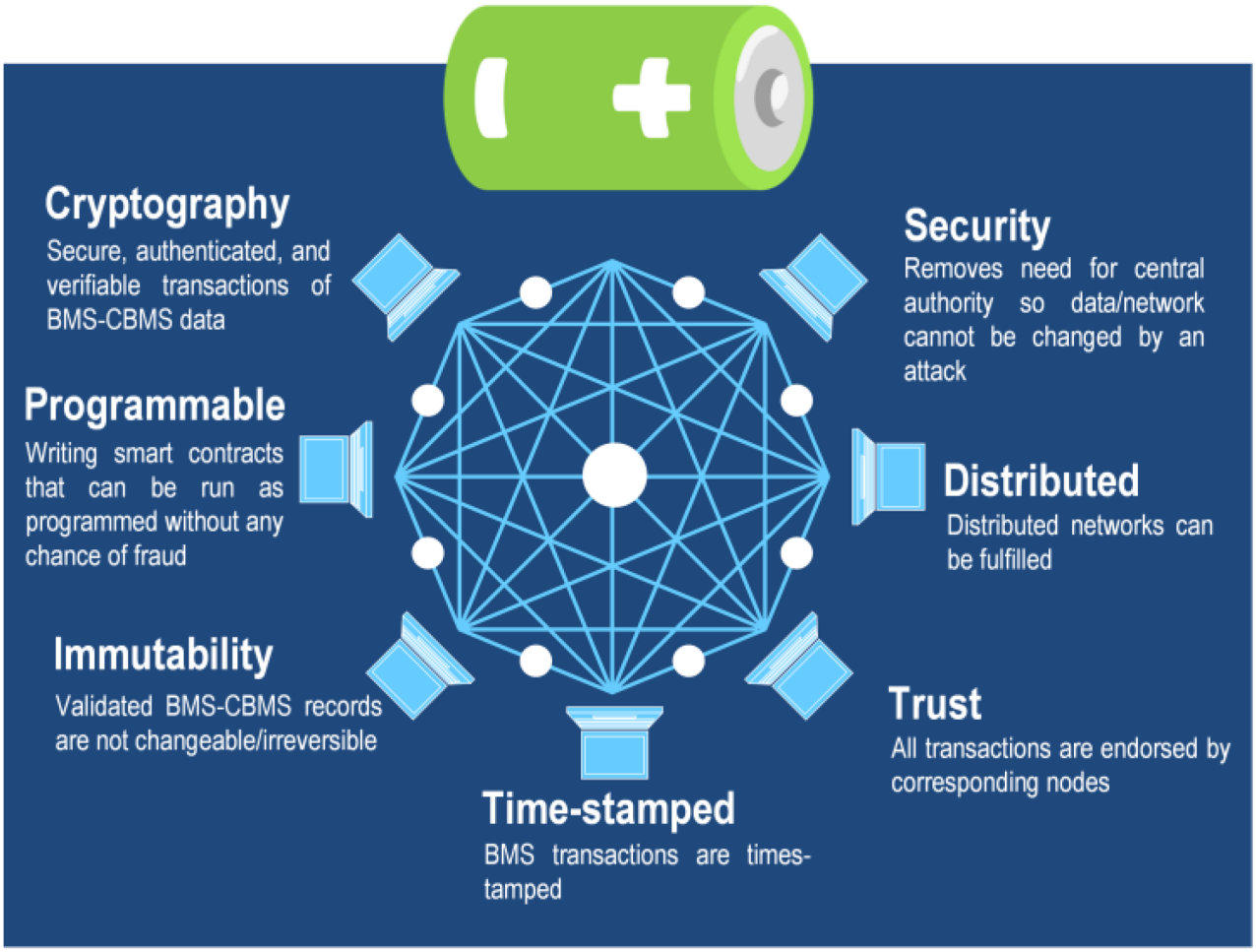

Figure 6. Main features of blockchain technology.

The application of blockchain in the CBMS context has been explored in several research papers. In [45], the Blockchain-as-a-Service (BaaS) concept was proposed for BESS applications. The main idea of BaaS is to develop a universal secure platform for CBMS implementation to support the implementation of a range of use cases. As suggested and conceptualized, the BaaS can be used to ensure the validity and integrity of battery data throughout the value chain. Other examples were presented in [46][47][48], where security-hardening technology and blockchain-based firmware security check and recovery frameworks were proposed for application to the (wireless) BMSs to enhance their cybersecurity. Similarly, Ref. [49] proposed a blockchain-based IoT network for the cybersecurity enhancement of wireless BMSs. A typical blockchain framework applied to the BMS context is shown in **Figure 7**.

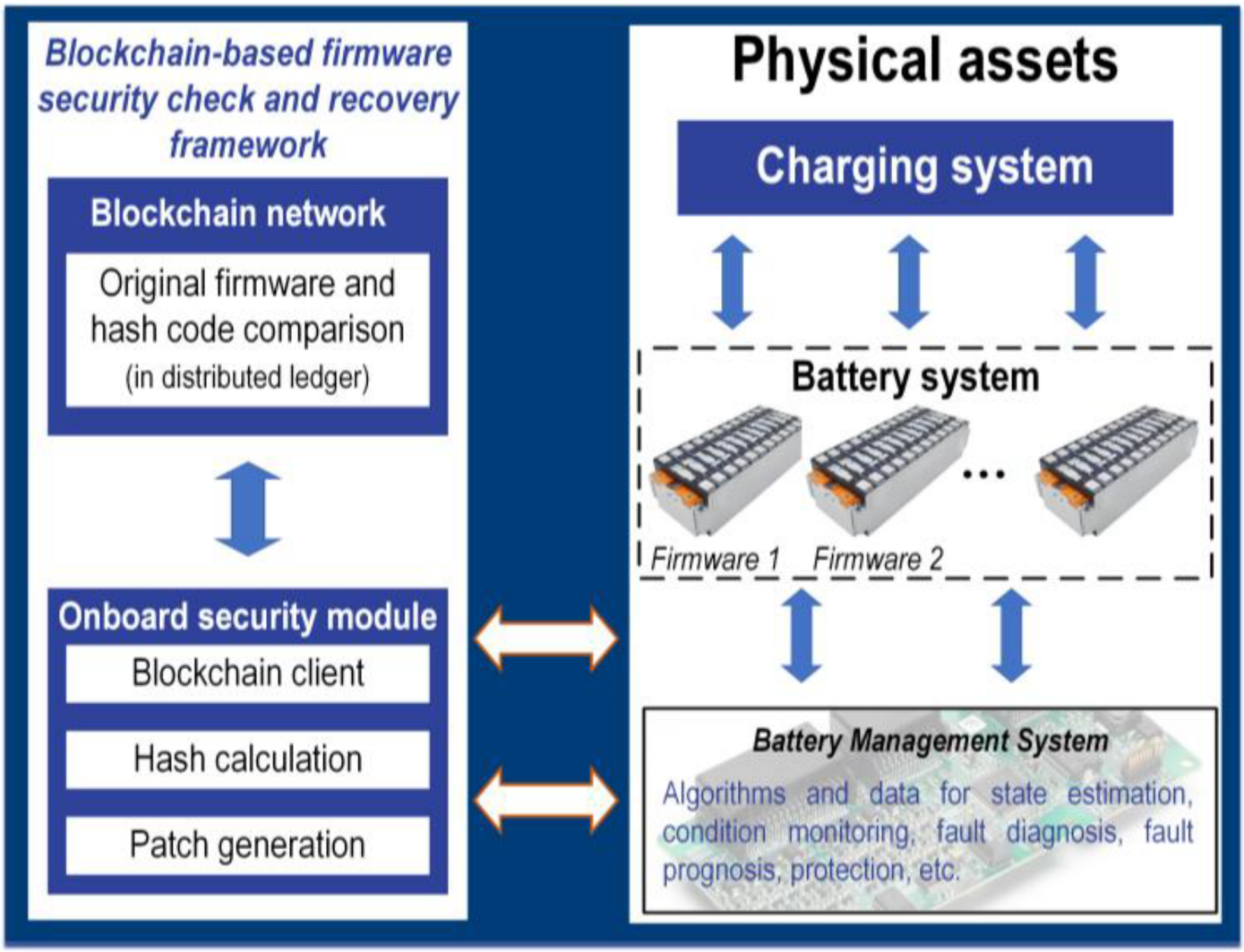

Figure 7. A typical architecture for blockchain-based firmware security enhancement [47].

The physical assets including the BMS units or charging equipment can be considered as a blockchain client. With hash calculation, each client will be given a unique fixed-size output that corresponds to a digital fingerprint of the input data. Any change to the input data will result in a different output hash, which can be used to check the authentication of the accesses to the database or codebase of the BMS [49]. Hash code comparison will be fulfilled in the distributed ledger, which means that hash codes will be stored and processed on a network rather than a single point. Thus, a high level of protection and security against all types of cyberattacks can be assured. A comprehensive discussion of the blockchain-based implementation of the battery control strategies on a distributed network of BMS nodes can be found in [23].

- *Resilient software design*: Design-for-cybersecurity (DFC) can be used to enhance the robustness of the CBMS software against cyberthreats. An example of DFC is the design of robust and resilient state estimation algorithms that are capable of detecting and/or neutralizing cyberattacks and their effects. Several CPS-based applications have reported the use of secure algorithms such as secure state estimators to protect against cyberattacks. For example, Refs. [50][51] designed a secure Kalman filter (KF)-based algorithm for dynamic state

estimation in energy grids. The algorithm was designed to detect the onset of an FDI attack and the location (specific communication nodes) where the attack was launched. Thus, with the resilient algorithm, the state estimations will recover to the true state estimates even though the measurements are manipulated. Another example was presented in [52], where a resilient algorithm was designed for finite-time secure state estimation in a centrifugal pump to protect it against sensor attacks. A resilient SOC estimation algorithm based on artificial neural networks (ANNs) was proposed in [53]. The algorithm was designed to neutralize the effect of cyberattacks on the battery data so the SOC estimations remain valid under attack conditions. Such techniques can be used to develop secure algorithms, for example, secure SoX estimation algorithms or cyberattack detection algorithms with the ability to discriminate between a failure (such as a sensor failure of cell failure) and a cyberattack. In this context, Ref. [11] highlighted the ability of AI-based data-driven methods in sensor measurement forecast (pseudo-measurement generation), which will offer redundancy for when the sensors are attacked. Similarly, Ref. [54] provided a few recommendations to enhance IoT-related security, e.g., through secure coding, formatting the source codes as libraries, executables, and obfuscation codes, which will prevent source code changes due to cyberattacks. As argued in [54], secure coding may refer to designing secure CBMS software together with a rule-checker for secure coding and an incorporated weakness analyzer. BMS software updates should also be performed securely. In this regard, researchers have suggested code-signing firmware updates [55]. The security of BMS source codes should also take into account reliable libraries throughout the source code [56].

- *Cross-verification of BMS and CBMS*: One potential solution to ensure the credibility of the CBMS algorithmic results such as SOX estimation results could be to perform the related calculations in different ways on both BMS and CBMS. The results obtained on the onboard BMS can then be used to cross-verify the accuracy of the CBMS algorithms and their robustness [25]. A great mismatch between the results of the onboard BMS and the CBMS potentially indicates an unusual situation such as a cyberattack launched against CBMS or IoT communication links.

- *Hardware Security Modules (HSMs)*: CPUs with security stacks and embedded HSMs are the nuclei of vehicle cybersecurity. They are used to protect safety-critical vehicle tasks such as the functioning of airbags, steering, and braking systems. Similarly, BMS processors can be protected against cyberthreats through the use of HSMs [57]. As shown, the HSM can be connected to the BMS microprocessor as separate hardware, which includes an individual processor, cryptographic functions, and dedicated memory to support hardware security firmware [57]. The BMS enhanced by HSM can perform autonomous authenticity and integrity checks, for example, when a software update is to be installed, for secure in-vehicle communications through the CAN bus, and in case of extra-vehicle communications to the IoT and CBMS. Reference [57] also suggested a procedure for the determination of the ASILs by including the cybersecurity risks in the functional safety analysis. Accordingly, it pinpoints the importance of end-to-end (E2E) protection for the exchange of critical data to ensure an ASIL D requirement, e.g., for data that are linked to the braking signals, steering angle, battery pack safety, etc.

- *Encryption*: Encryption refers to the process of encoding BMS/CBMS software data/information to prevent unauthorized access and/or data alternation [58]. Encryption can help ensure that sensitive battery/BMS data is

kept confidential and that only authorized assets have access to the data. Internal communications, such as communication from slave boards to master BMS or vehicle CAN communication, as well as IoT communications from BMS to the CBMS and vice versa, can be effectively protected using cryptographic protocols such as TLS [54]. For example, end-to-end encryption based on NISTIR guidance on cryptography and key management has been suggested to assure the integrity and confidentiality of battery data [59][60]. Likewise, to protect against MitM cyberattacks, additional end-point security protocols (such as IEC 62351-7) and role-based access control (RBAC) based on IEC 62351-8 can be considered [61]. Regarding different battery data stored on CBMS, database encryption is an effective solution to prevent data stealth. Database encryption transfers different battery data (state data, link data, metadata, etc.) into cipher text which cannot be comprehended by unauthorized users (e.g., by attackers). Examples of database encryption methods are the hashing technique, SHA256 encryption, etc. [54]. In this regard, the National Renewable Energy Laboratory (NREL) also highlights the effectiveness of encryption in protecting both data-at-rest (data stored on BMS and/or CBMS) and data-in-flight (battery transactions real-time data) [29]. Despite being a powerful solution, encryption has some weaknesses. Encryption requires key management to encrypt and decrypt data or codes, and if the key is stolen, intercepted, or compromised, the data encryption can be broken. To ensure key security, Ref. [62] suggested a pluggable key management device with a key management protocol and integrated formal analysis to assure security compliance. It is also noteworthy that encryption protocols and algorithms are somehow susceptible to vulnerabilities such as side-channel attacks. Moreover, encryption is useless in the case of specific attack types against CBMS such as random delay attacks.

- *User authentication and access control* [63][64]: User authentication provides an additional layer of security against unauthorized access to the battery, CBMS, and related data. Multifactor authentication or passwords can be used when accessing the battery database on the cloud, CAN bus through the OBD port, before performing maintenance, or when configuration/reconfiguration of the BMS or CBMS software is planned. Adopting ISO 15118 multimodal and multipass authentication processes was suggested in [65]. Likewise, in the case of adopting the MQTT protocol for IoT communications, Ref. [54] suggested that access to the broker should be restricted by deploying authentication keys on both sides including the clients and broker. In this context, Ref. [54] recommended using proper tools for checking the login history to track unauthorized access attempts.

In addition to the aforementioned protection mechanisms, physical protection of the communication terminals/nodes, e.g., through secure housing designs, hardwiring, etc., should also be considered a priority in the design of the BMS/CBMS components [25]. NREL recommends removing BMS unnecessary interfaces and external ports, adding tamper monitoring and resistance [66], adding secure bootloaders to BMS, removing hard-coded passwords, and certification of CBMS services with the Federal Risk and Authorization Management Program (FedRAMP) [7]. For example, one can refer to a recent project which investigates a so-called s-NIC card (Secure NETWORK Interface Card) that supports secure boot and tamper resistance for EVSE applications [67]. Likewise, Refs. [11][25] highlighted the importance of transparency in battery data and algorithms to secure processes related to testing, verifying, and communicating between BMS and CBMS. This is important to improve the explainability of data/algorithms, since, usually, many factors affect the balance and optimization of algorithms'

performances. Transparency reduces the cybersecurity risk by maintaining human-in-the-loop, which will make cyberattacks more apparent before they turn into a risk [25].

DFC requires additional effort for designing and implementing proper cybersecurity measures. Thus, the overall cost of the system will be increased. The optimum cybersecurity practice should thus be chosen based on the application area, specific use cases of the CBMS, and the implementation strategy, such as how the BMS and CBMS will talk to each other and how CBMS feedback will be prioritized. Multiple security measures can be simultaneously adopted if a high-security level is demanded.

In the context of digital twins, a detailed review of threats and cybersecurity recommendations were presented in [68]. **Table 1** provides a summary of key CBMS cybersecurity topics discussed in this section.

Table 1. Summary of the key issues related to CBMS cybersecurity.

Potential Attack Paths		Impacts on CBMS	Countermeasures
▪ **EV:** Against CAN bus interfaces, wireless communication between CSUs and PMU, sensors, meters, ports (OBD-II, USB, etc.). ▪ **EVSE and battery swapping stations:** High risk of physical manipulation; communication line between EV and EVSE; in case of V2X, communication links between EVSE, charge station operators/aggregators, and grid operator. ▪ **IoT communication:** Against communication links from BMS to CBMS with different protocols, e.g., MQTT, TCP/IP, Wi-Fi, Bluetooth, Zigbee, etc. ▪ **CBMS:** Against cloud infrastructure (CBMS accounts on the cloud, databases, APIs, etc.).		▪ **Functional impacts:** Attacks impacting operation of subsystems, systems, components, functions, or algorithms in CBMS. Examples are denial-of-charging, divergence of SoX algorithms, suboptimal operation of thermal and energy management systems, etc. ▪ **Financial loss:** BMS malfunctioning resulting in accelerated degradation of the battery. Falsified SoH data leading to wrong battery maintenance exercises (too soon or too late). ▪ **Safety impacts:** BMS malicious firmware updates resulting in	▪ **Blockchain:** Protects critical CBMS activities related to storage, sharing, and transactions of battery-related data. Blockchain-protected CBMS data cannot be accessed or changed by any unauthorized parties. ▪ **Encryption:** Encoding CBMS software data and information to prevent unauthorized access and malicious alteration. Protocols such as TLS for end-to-end encryption can be applied. In addition to communication encryption, the CBMS database can be encrypted to protect against storage attacks. ▪ **Resilient software design:** Practices include resilient
Potential cyberattacks against CBMSs			
Confidentiality	▪ **Sniffing (snooping) attack:** Attacker		

Potential Attack Paths		Impacts on CBMS	Countermeasures
	passively listens to the data traffic. ▪ **MitM attack:** Attacker might also have the possibility to affect the data flow. ▪ Stolen information can be used to construct more complicated attack scenarios.	battery exceeding its limits leading to overcharge, overdischarge, etc. Overcharge resulting in accelerated aging. Overcharge in the scale of minutes causing risks of internal short-circuits and thermal runaways. Cooling system performance becoming compromised leading to the thermal runaway risk. Poor estimation of SoX data might result in lower safety. There is also a safety risk if the battery pack is disconnected, or its performance is limited due to a cyberattack while the EV is in driving mode. ▪ **Privacy:** Technology and intellectual property theft, disclosed private information, e.g., GPS data. ▪ **Side impacts:** CBMS database poisoning can corrupt subsequent battery and BMS designs that are fulfilled based on the attacked datasets.	algorithm design such as robust SoX estimators, secure coding, formatting source codes as libraries, executables, and obfuscation codes, securing BMS software updates, etc. ▪ **HSM:** Connects to the BMS as separate hardware and includes an individual processor, cryptographic functions, and dedicated memory to support hardware security firmware. ▪ **Authentication:** Provides an additional layer of security against unauthorized access to the CBMS and related data. Multifactor authentication, multimodal, and multipass authentication processes have been suggested. ▪ **Cross-validation:** Checks processing/algorithmic results on both BMS and CBMS and compares them. Big mismatches can be signs of cyberattacks. ▪ **Physical protection:** Secure housing design, hardwiring, removing unnecessary interfaces and external ports, etc. ▪
Integrity	▪ **FDI:** Refers to deliberate manipulation of the CBMS data/measurements by injecting false data vectors to the original data. ▪ **Random delay attack:** A delay will be deliberately introduced to the sequence of BMS control commands or data. ▪ **Replay attack:** Wiretapping and repeatedly broadcasting the battery/CBMS measurements/data.	Attack Detection	

Potential Attack Paths		Impacts on CBMS	Countermeasures
Availability	▪ **Flooding:** DoS attacks buffering too much information toward the IoT, causing it to slow down. ▪ **Crashing:** When the DoS attack aims to stop CBMS services. ▪ **EMI attack:** Malicious EMI source disrupting wireless link between CMUs and PMU.	▪ **IDS:** Monitoring traffic of CBMS network and comparing to known traffic patterns under different attack types. ▪ **Behavior-based detection:** Monitoring and comparing behavior of signals (current, voltage, etc.) and comparing them to a baseline to create detection residual signals. ▪ **ML-based methods:** Using ML to distinguish between data patterns in attacked and nonattacked conditions.	**Data and algorithm transparency:** Reduces the cybersecurity risk by maintaining human-in-the-loop, which will make cyberattacks more apparent before they turn into a risk.

3. Sanghvi, A.; Markel, T. Cybersecurity for electric vehicle fast-charging infrastructure. In Proceedings of the 2021 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 21–25 June 2021; pp. 573–576.
4. Metere, R.; Pourmirza, Z.; Walker, S.; Neaimeh, M. An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure. arXiv 2022, arXiv:2209.07842.
5. Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of smart electric vehicle charging: A power grid perspective. IEEE Access 2020, 8, 214434–214453.
6. Park, Y.; Onar, O.C.; Ozpineci, B. Potential cybersecurity issues of fast charging stations with quantitative severity analysis. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; pp. 1–7.
7. Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies 2022, 15, 3931.
8. Bharathidasan, M.; Indragandhi, V.; Suresh, V.; Jasiński, M.; Leonowicz, Z. A review on electric vehicle: Technologies, energy trading, and cyber security. Energy Rep. 2022, 8, 9662–9685.
9. ISO 15118-20:2022. Road Vehicles—Vehicle to Grid Communication Interface. 2022. Available online: https://www.iso.org/standard/77845.html (accessed on 21 May 2023).

10. Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and countermeasures. IEEE Access 2020, 8, 226982–226998.
11. Kharlamova, N.; Hashemi, S.; Træholt, C. Data-driven approaches for cyber defense of battery energy storage systems. Energy AI 2021, 5, 100095.
12. Johnson, J.; Hoaglund, J.R.; Trevizan, R.D.; Nguyen, T.A. Physical Security and Cybersecurity of Energy Storage Systems. In U.S. DOE Energy Storage Handbook; Sandia National Laboratories: Albuquerque, NM, USA, 2020.
13. Maheshwari, P.U.; Bhargavi, S.; Umarani, S. Advancements in Cyber Security for Autonomous Vehicles. Int. J. Wirel. Netw. Secur. 2021, 7, 33–40.
14. Tran-Jørgensen, P.W.; Kulik, T.; Boudjadar, J.; Larsen, P.G. Security analysis of cloud-connected industrial control systems using combinatorial testing. In Proceedings of the 17th ACM-IEEE International Conference on Formal Methods and Models for System Design, La Jolla, CA, USA, 9–11 October 2019; pp. 1–11.
15. Kulik, T.; Larsen, P.G. Extensions to Formal Security Modeling Framework. 2018. Available online: https://github.com/kuliktomas/FCSVIoT/commit/189c7962f7f0870fa5315c31a71a6b35e896e47d (accessed on 3 June 2023).
16. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics 2022, 11, 16.
17. Kulik, T.; Gomes, C.; Macedo, H.D.; Hallerstede, S.; Larsen, P.G. Towards secure digital twins. In Leveraging Applications of Formal Methods, Verification and Validation, Proceedings of the 11th International Symposium, ISoLA 2022, Rhodes, Greece, 22–30 October 2022; Springer: Berlin/Heidelberg, Germany, 2022; Part IV; pp. 159–176.
18. Kharlamova, N.; Hashemi, S.; Træholt, C. The cyber security of battery energy storage systems and adoption of data-driven methods. In Proceedings of the 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Laguna Hills, CA, USA, 9–13 December 2020; pp. 188–192.
19. Krishna, G.; Singh, R.; Gehlot, A.; Akram, S.V.; Priyadarshi, N.; Twala, B. Digital Technology Implementation in Battery-Management Systems for Sustainable Energy Storage: Review, Challenges, and Recommendations. Electronics 2022, 11, 2695.
20. Gonzalez, I.; Calderón, A.J.; Folgado, F.J. IoT real time system for monitoring lithium-ion battery long-term operation in microgrids. J. Energy Storage 2022, 51, 104596.
21. Alzahrani, A.; Wangikar, S.M.; Indragandhi, V.; Singh, R.R.; Subramaniyaswamy, V. Design and Implementation of SAE J1939 and Modbus Communication Protocols for Electric Vehicle. Machines 2023, 11, 201.

22. Yang, S.; Liu, X.; Li, S.; Zhang, C. Advanced Battery Management System for Electric Vehicles; Springer Nature: Berlin/Heidelberg, Germany, 2022.
23. Mhaisen, N.; Fetais, N.; Massoud, A. Secure smart contract-enabled control of battery energy storage systems against cyber-attacks. Alex. Eng. J. 2019, 58, 1291–1300.
24. Guo, L.; Yang, B.; Ye, J.; Chen, H.; Li, F.; Song, W.; Du, L.; Guan, L. Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles. IEEE Trans. Ind. Inform. 2020, 17, 3335–3347.
25. Madeline, C.; Richard, S. Cybersecurity of Battery Management Systems. In Readout: Horiba Technical Reports; HORIBA: Singapore, 2019; pp. 82–89.
26. Rohde, K.W. Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid; Idaho National Lab. (INL): Idaho Falls, ID, USA, 2019.
27. Sripad, S.; Kulandaivel, S.; Pande, V.; Sekar, V.; Viswanathan, V. Vulnerabilities of electric vehicle battery packs to cyberattacks. arXiv 2017, arXiv:1711.04822.
28. Eiza, M.H.; Ni, Q. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. IEEE Veh. Technol. Mag. 2017, 12, 45–51.
29. Hodge, C.; Hauck, K.; Gupta, S.; Bennett, J.C. Vehicle Cybersecurity Threats and Mitigation Approaches; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2019.
30. Idaho National Laboratory. Cyber Security Research and Development: Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment; Idaho National Laboratory: Hong Kong, China, 2018.
31. Acharya, S.; Dvorkin, Y.; Karri, R. Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable? IEEE Trans. Smart Grid 2020, 11, 5099–5113.
32. Morrison, G.S. Threats and Mitigation of DDoS Cyberattacks Against the US Power Grid via EV Charging. Master’s Thesis, Wright State University, Dayton, OH, USA, 2018.
33. Johnson, J.; Anderson, B.; Wright, B.; Graves, R.; Daley, J.; Quiroz, J.; Pratt, R.; Carroll, T.; O’Neil, L.; Dindlebeck, B. Securing Electric Vehicle Charging Infrastructure—Final Report; Sandia National Laboratory: Albuquerque, NM, USA, 2021.
34. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B.; David, R.P.; Machado, R.C.S. Artificial neural network-based stealth attack on battery energy storage systems. IEEE Trans. Smart Grid 2021, 12, 5310–5321.
35. Kong, W.W.; Luo, Y.; Qi, Y.; Wang, Y. Full Protection Scheme and Energy Optimization Management of the Battery in Internal Combustion Engine Vehicles Based on Power Partitioning Model; SAE Technical Paper; SAE International: Warrendale, PA, USA, 2019; ISSN 0148-7191.

36. Xie, J.; Chen, J.; Li, L.; Chen, Y. Advanced Battery Early Warning and Monitoring System. U.S. Patent US9177466B2, 3 November 2015.
37. Liao, H.-J.; Lin, C.-H.R.; Lin, Y.-C.; Tung, K.-Y. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 2013, 36, 16–24.
38. Junejo, K.N.; Goh, J. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an, China, 30 May 2016; pp. 34–43.
39. Lee, H.; Bere, G.; Kim, K.; Ochoa, J.J.; Park, J.-H.; Kim, T. Deep learning-based false sensor data detection for battery energy storage systems. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6.
40. Dey, S.; Khanra, M. Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging. IEEE Trans. Ind. Electron. 2020, 68, 478–487.
41. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet 2020, 12, 157.
42. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics 2022, 11, 198.
43. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics 2022, 11, 1502.
44. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, H.A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. 2020, 10, 1270–1281.
45. Ochoa, J.J.; Bere, G.; Aenugu, I.R.; Kim, T.; Choo, K.-K.R. Blockchain-as-a-Service (BaaS) for battery energy storage systems. In Proceedings of the 2020 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 6–7 February 2020; pp. 1–6.
46. Ochoa, J. Security-Enhanced Cyber-Physical Battery Management System Using Blockchain and Security Hardening Technology; Texas A&M University: Kingsville, TX, USA, 2020.
47. Bere, G.; Ochoa, J.J.; Kim, T.; Aenugu, I.R. Blockchain-based firmware security check and recovery for battery management systems. In Proceedings of the 2020 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 23–26 June 2020; pp. 262–266.
48. Liu, M.; Yeoh, W.; Jiang, F.; Choo, K.-K.R. Blockchain for Cybersecurity: Systematic Literature Review and Classification. J. Comput. Inf. Syst. 2022, 62, 1182–1198.

49. Faika, T.; Kim, T.; Ochoa, J.; Khan, M.; Park, S.-W.; Leung, C.S. A blockchain-based Internet of Things (IoT) network for security-enhanced wireless battery management systems. In Proceedings of the 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 29 September–3 October 2019; pp. 1–6.
50. Kazemi, Z.; Safavi, A.A.; Naseri, F.; Urbas, L.; Setoodeh, P. A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks. IEEE Trans. Ind. Inform. 2020, 16, 7275–7286.
51. Kazemi, Z.; Safavi, A.A.; Setoodeh, P. Efficient resilient dynamic co-estimation framework for cyber-physical systems under sensor attacks. IET Control Theory Appl. 2020, 14, 3526–3536.
52. Kazemi, Z.; Safavi, A.A.; Arefi, M.M.; Naseri, F. Finite-Time Secure Dynamic State Estimation for Cyber–Physical Systems Under Unknown Inputs and Sensor Attacks. IEEE Trans. Syst. Man Cybern. Syst. 2021, 52, 4950–4959.
53. Rahman, S.; Aburub, H.; Mekonnen, Y.; Sarwat, A.I. A study of EV BMS cyber security based on neural network SOC prediction. In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Denver, CO, USA, 16–19 April 2018; pp. 1–5.
54. Kumbhar, S.; Faika, T.; Makwana, D.; Kim, T.; Lee, Y. Cybersecurity for battery management systems in cyber-physical environments. In Proceedings of the 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, USA, 13–15 June 2018; pp. 934–938.
55. Stykas, V. Smart Car Chargers. Plug-n-Play for Hackers. 2021. Available online: https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/ (accessed on 3 June 2023).
56. Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, A.I. Facts approach to address cybersecurity issues in electric vehicle battery systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 12–14 June 2019; pp. 1–6.
57. Bierbaum, D.; Stampa, R. Smart Synthesis of Cybersecurity and Functional Safety. ATZelectron. Worldw. 2021, 16, 8–11.
58. Kulik, T.; Dongol, B.; Larsen, P.G.; Macedo, H.D.; Schneider, S.; Tran-Jørgensen, P.W.; Woodcock, J. A survey of practical formal methods for security. Form. Asp. Comput. 2022, 34, 1–39.
59. van Eekelen, M.; Poll, E.; Hubbers, E.; Vieira, B.; van den Broek, F. An End-to-End Security Design for Smart EV-Charging for Enexis and ElaadNL; ElaadNL: Arnhem, The Netherlands, 2014.

60. Pillitteri, Y.V.; Brewer, L.T. NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity; Smart Grid Interoperability Panel (SGIP): Gaithersburg, MD, USA, 2014; p. 668.
61. Rubio, J.E.; Alcaraz, C.; Lopez, J. Addressing security in OCPP: Protection against man-in-the-middle attacks. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
62. Ubys, L.; Nicolas Vancea, V.; Kulik, T.; Gorm Larsen, P.; Boudjadar, J.; Aranha, D.F. Formal Model In-The-Loop for Secure Industrial Control Networks. In Proceedings of the Formal Aspects of Component Software: 18th International Conference, FACS 2022, Virtual Event, 10–11 November 2022; pp. 74–89.
63. ElaadNL. Security Architecture for Electric Vehicle Charging Infrastructure, Version 1.0; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
64. ElaadNL. Security Architecture for Electric Vehicle Charging Infrastructure, Version 2.0; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
65. Vaidya, B.; Mouftah, H.T. Multimodal and multi-pass authentication mechanisms for electric vehicle charging networks. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 371–376.
66. Gottumukkala, R.; Merchant, R.; Tauzin, A.; Leon, K.; Roche, A.; Darby, P. Cyber-physical system security of vehicle charging stations. In Proceedings of the 2019 IEEE Green Technologies Conference (GreenTech), Lafayette, LA, USA, 3–6 April 2019; pp. 1–5.
67. Chhaya, S.; Ghatikar, R. Cybersecurity Platform and Certification Framework Development for EXtreme Fast Charging (XFC) Infrastructure Ecosystem. In Proceedings of the DOE Vehicle Technologies Office Annual Merit Review; Electric Power Research Institute, Inc.: Washington, DC, USA, 2021.
68. Alcaraz, C.; Lopez, J. Digital twin: A comprehensive survey of security threats. IEEE Commun. Surv. Tutor. 2022, 24, 1475–1503.