Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects

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

Published in:
Batteries

DOI (link to publication from Publisher):
10.3390/batteries9070382

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

batteries

MDPI

Review

Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects

Farshid Naseri [1,*], Zahra Kazemi [2], Peter Gorm Larsen [2], Mohammad Mehdi Arefi [3] and Erik Schaltz [1,*]

[1] Department of Energy, Aalborg University, 9220 Aalborg, Denmark
[2] Department of Electrical and Computer Engineering, Aarhus University, 8200 Aarhus, Denmark
[3] Department of Power and Control Engineering, Shiraz University, Shiraz 71348-14336, Iran
* Correspondence: fna@energy.aau.dk (F.N.); esc@energy.aau.dk (E.S.)

Abstract: 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. Recently, 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. However, as for any other CPS, the CBMS creates vulnerabilities against cyberattacks and if not properly secured, could end up damaging the BESS and/or causing dangerous, expensive, and life-threatening situations. Cybersecurity of the CBMSs has thus become a trending topic and several works have been published in this area in recent years. This paper conducts a scoping review to address different topics related to BMS cybersecurity. The CBMS architecture is presented, and the potential cyberattack surfaces are identified. Different possible attack scenarios, including attack points, attack types, and their impact at the component level (BMS and BESS) and system level (vehicle or grid), are discussed. In addition, the paper provides a review of potential countermeasures to protect the CBMS against cyberattacks. The paper also includes a review of the applicable standards and regulations that relate to this trending topic. Finally, based on the reviewed gaps, potential future research domains on BMS cybersecurity topics are identified and presented at the end of the paper.

Keywords: electric vehicle; battery management systems; cloud computing; cybersecurity; cyberattacks; blockchain; cyber-physical systems; Internet of Things; machine learning; artificial intelligence

Citation: Naseri, F.; Kazemi, Z.; Larsen, P.G.; Arefi, M.M.; Schaltz, E. Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects. *Batteries* **2023**, *9*, 382. https://doi.org/10.3390/batteries9070382

Academic Editor: Federico Baronti

Received: 2 June 2023
Revised: 5 July 2023
Accepted: 13 July 2023
Published: 18 July 2023

1. Introduction

Large investments are expected to reach the automotive sector to produce electric vehicles (EVs) and EV supply equipment (EVSE) in the coming decade. As such, the energy storage industry has witnessed tremendous growth to support transportation electrification. The battery industry has also experienced significant technological advancements related to different aspects of batteries from cell production to module and pack design and assembly. A particularly important element in the battery pack is the battery management system (BMS), which is critically linked to EV functional safety. The BMS refers to the electronics and software that are designed to function the battery pack within safe and efficient operating windows [1]. The BMS is usually implemented into the pack onboard the EV and it normally contains (as an integrated unit) hardware and software to monitor, protect, and control the operation of the battery pack [2]. The performance of the BMS has a direct impact on the EV on the road in terms of its driving range, charging speed, maintenance, the longevity of the battery, safety, etc. The lithium-ion (Li-ion) batteries

used in EVs have complex system characteristics, i.e., they are dynamic, nonlinear, time-variant, and can be thermally unstable [3]. Likewise, no two cells in a pack are alike and these cell-to-cell variations complicate the BMS design [4]. It is, thus, challenging to develop high-performance models and algorithms to adapt the complex cell behaviors in a pack. Significant research effort has been dedicated to improving the BMS performance by developing more advanced and efficient BMS algorithms for energy management [5], fault diagnosis, state-of-X (SOX) estimation where X may refer to charge (SOC), health (SOH), or power (SOP) [6], etc.

Another challenge is that the performance of the onboard BMS is usually confined by the limited available processing power associated with the integrated microprocessor [7]. Generally, the BMS integrated processing power is limited to a few hundred Mbytes [8] to maintain its price competitiveness. The CPU/memory is allocated to execute various BMS functions related to fault diagnosis, protection, cell balancing, and SOX estimation. Likewise, many of the BMS algorithms should be simultaneously implemented for a large number of cells within the battery pack and should be executed in parallel, which will significantly increase the computational requirements. This will place a limit on the complexity level of the BMS algorithms to ensure the feasibility of embedded implementation. As a result, the best-in-class algorithms cannot often be implemented in the onboard BMS due to their complexity. For example, artificial intelligence (AI) and machine learning (ML)-based algorithms require access to massive amounts of vehicle/battery historical data, which are difficult to store/process using the onboard BMS due to the limited processing power [9]. Although the use of advanced physics-based battery models has shown promising results to improve algorithmic performance such as accuracy in SOH prediction [10], their implementation in BMS is usually hindered by the lack of sufficient computational resources. Thus, in practice, only simple models with reduced performance such as equivalent circuit models (ECMs) are considered in the BMS context. Increasing the BMS computational capacity results in additional costs and reduces the affordability of EVs.

To address these shortcomings, the concept of the Cloud BMS (CBMS) was recently proposed [4]. The CBMS is a cyber-physical BMS combining different technologies including cloud computing, AI, and Internet of Things (IoT). The idea of the CBMS is to use IoT to transmit battery data to the cloud to undertake heavy BMS computations such as running advanced digital twin physics-based models, storing, and processing big data to predict the states of the battery, etc. [4]. This way the BMS can learn from past data to provide more accurate future state predictions. In principle, these cloud services can be potentially shared among more than one battery pack or EV, which will result in enhanced cost-effectiveness. It has thus been argued that the CBMS concept enhances scalability and adaptability [11], in addition to higher battery performance achievable in terms of safety, reliability, and flexibility by using best-in-class algorithms on the cloud [4].

The CBMS concept is relatively new, and to the authors' best knowledge has only been validated up to a technology readiness level (TRL) of 5–6. However, some specific use cases of the CBMSs have already reached the market. Pushing toward higher TRL levels and wider adoption of the CBMSs requires more studies and investigations of different aspects of the technology to ensure functional safety, as required by ISO26262 [12]. One critical aspect is security. The CBMS is a cyber-physical system (CPS) and, similar to any other CPS, is subjected to cyber and/or physical vulnerabilities. The BMS internal or external communications through the controller area network (CAN) or IoT communications potentially create malicious attack risk. Successful attacks can manipulate BMS algorithms, control signals, or sensing data of the battery, which can lead to battery degradation, damage, or fire. Therefore, the security of the CBMS has to be carefully analyzed to ensure functional safety. This includes exploration of potential attack points, scenarios, and analysis of impacts on the battery system and EV as a whole. Likewise, actions that must be taken to prevent and control the security risks have to be discussed.

A comprehensive review of papers and relevant standards published on this subject is carried out in this paper and, accordingly, different aspects of CBMS cybersecurity are

discussed in detail. Potential attack paths and scenarios are identified and their impact on the subsystem (BESS) and system (EV or grid) levels are assessed. Likewise, methods that can be used for the detection of cyberattacks and for improving CBMS cybersecurity are presented. The paper further contributes to the review of existing standards/regulations related to the subject. According to the identified research and industrialization gaps, the paper also provides recommendations about potential research domains that are worthy to explore in the future to advance CBMS cybersecurity. It should be noted that the analysis in this paper is centered mostly around vehicular BMSs; however, the majority of discussions apply to CBMSs for stationary (grid) BESSs as well. Thus, topics related to the cybersecurity of EVSEs, V2G cybersecurity, etc., are also covered in this paper to some extent.

The rest of this paper is organized as follows: In Section 2, the review methodology is described and some statistics about the literature database are presented. Section 3 provides a general overview of the CBMS and related functionalities and requirements. In Section 4, different aspects related to the CBMS cybersecurity, including potential cyberattack surface, cyberattack scenarios, and impacts on the performance, are discussed. Likewise, some potential countermeasures to improve the security of the CBMS are suggested. Different existing standards and regulations that relate to CBMS cybersecurity are surveyed in Section 5. In Section 6, gaps and potential future research domains are presented and discussed. Finally, the review is concluded in Section 7.

2. Literature Analysis

The literature search was fulfilled based on Scopus and IEEE Xplore scientific databases. Gray literature (according to Google Scholar search) was also considered in the search process to complement the databases. The publication types considered include peer-reviewed articles (both in journals and conference proceedings), book chapters, dissertations, and theses, as well as technical reports. As for the search period, all research published between 2000–2023 was taken into account. Only the literature in English was analyzed. The search settings, including the search strings and keywords, are summarized in Table 1.

Table 1. Summary of the search settings.

Search Index	Specific Content
Database	Scopus, IEEE Xplore, gray literature.
Publication Type	Peer-reviewed journal and conference articles, book chapters, technical reports, dissertations/theses.
Search Strings	"cloud battery management system", "cloud BMS", "battery digital twin", "battery cybersecurity", "vehicle cybersecurity", "battery security".
Search Period	2000–2023.

The classification per publication year is shown in the histogram chart of Figure 1. As the chart shows, the first work fulfilled on CBMS cybersecurity was published in 2015 while the number of publications on this subject has been steadily increasing, which shows that this is a timely topic. The growing number of publications in recent years also shows the pertinence of this review paper and that it is timely.

The classification of the publication types is also depicted in Figure 2, which shows that 78% of the publications are journal and conference articles, 12% are related to technical reports, and the rest includes book chapters, dissertations, and other publications, e.g., preprints, etc.

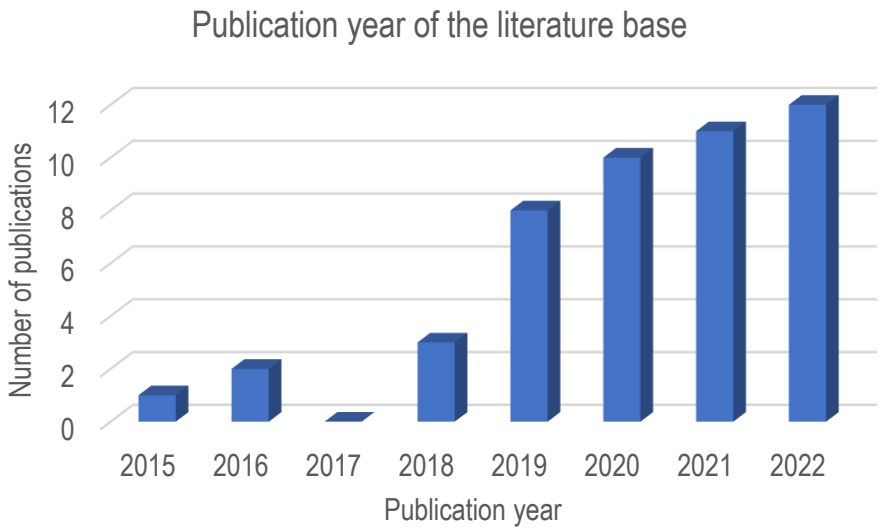

Figure 1. Publication year of the reviewed literature base.

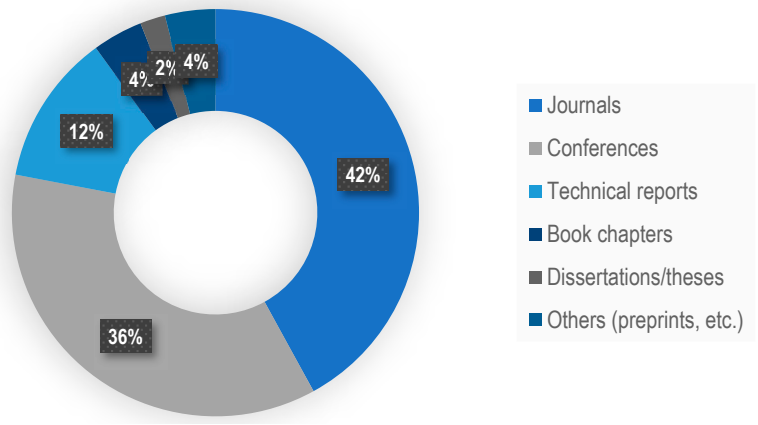

Figure 2. Percentage of each publication type in the analyzed literature base.

The contents of the collected literature database are carefully analyzed to compile information for different sections of this review paper. The literature review results are presented throughout the following sections.

3. BMS versus CBMS: Overview of Characteristics and Architectures

Li-ion battery cells have limited voltage, energy, and power. Thus, battery packs of EVs are built up from hundreds to thousands of battery cells connected in series and parallel to reach the required voltage, power, and energy levels. In practice, cell-to-cell variations usually exist in a pack, which can be imposed internally or externally. The internal cell-to-cell variation refers to the differences in cell characteristics such as the capacity and internal resistances originating from imperfect manufacturing processes [13]. These small cell-to-cell variations can grow larger due to poor external operating conditions such as uneven cooling of cells which will result in different aging patterns among cells. The inhomogeneity in the cells' characteristics and operation reduces the safety and performance of the pack. Cells with lower capacity tend to be charged or discharged faster and, thus, capacity inconsistencies can result in some cells being overcharged or overdischarged, thereby creating the risk of thermal runaway and battery fires [14]. Likewise, the performance of the pack will be limited by the lowest-capacity cell, which means the energy stored in cells/pack will not be utilized to its full advantage.

To tackle the aforementioned challenges, it is critical to equip the battery pack with a BMS. In the EV battery pack, the BMS fulfills the following roles:

- Ensuring protection and safety: The BMS measures and monitors the key variables related to the battery cells, including current, voltage, and temperature. It is also responsible for maintaining these variables within safe operating limits during charging and discharging. If, for any reason, the battery cannot be controlled within the critical safety limits, the BMS must send a command to the main contactor to shut off the battery pack. The BMS also measures the leakage current from the battery to protect against electrocution in case battery pack isolation is lost [15].
- Battery state estimation and monitoring: The internal states of Li-ion batteries cannot be quantified without any physical sensor. Thus, the BMS integrates algorithms to estimate the SoX parameters related to SoC, SoH, and SoP. The estimation data determine the operational boundaries of the cells such as the usable energy, remaining life, and feasible and safe charge/discharge power limits. Likewise, this information will be communicated to the vehicle's user interface and/or extended algorithms in the vehicle's electronic control unit (ECU).
- Controlling the battery: The battery pack is usually equipped with several actuators to control the operation of the battery, e.g., a precharge contactor to mitigate the inrush current drawn from the battery when connected to a charger, two contactors on positive and negative terminals to disconnect and isolate the battery pack in case of failure or maintenance work, MOSFET switches to control the voltage/SoC balancing between cascaded cells, etc. The BMS is responsible for continuously monitoring the battery pack and sending necessary control signals to activate/deactivate the actuators in different operating conditions of the battery.
- Condition monitoring and fault diagnosis: The BMS will continuously monitor the battery for anomalies. The battery anomalies include overvoltage, overcharge, overdischarge, unusual temperature conditions, outgassing, overcurrent, internal or external short-circuits in cells, failures in sensors or communication links that carry on critical cell data, etc.

The BMS is usually an integrated unit of software and hardware components. The most common BMS hardware architecture is the modular or master–slave BMS. The topology consists of slave boards named cell monitoring units (CMUs) and a master board named pack monitoring unit (PMU) [16]. The CMUs integrate the sensing ICs, balancing resistors/MOSFETs for passive/active cell balancing, and logic to protect against failures. One CMU can generally handle a unit of up to 16–18 series connected cells. Multiple CMUs can be used when a higher number of cells should be handled. The PMU integrates the main processor where complex BMS algorithms should run. Most commonly, the CMUs are connected with wires to the PMU in a daisy chain of twisted-pair cabling, which carries cell VIT (voltage, current, temperature) measurements back to the PMU with stringent safety requirements and ASIL D (Automotive Safety Integrated Level D) compliance. Alternative communication protocols from CMU and PMUs are based on RS485, I2C, or SPI. In the new generation of the BMSs, the communication between CMUs and the PMU is sometimes fulfilled via wireless communication [16]. It has been argued that BMS wireless communication improves reliability and reduces design complexity by simplifying the wiring harness, removing wires, and isolation connectors [16]. Likewise, it reduces the manufacturing and assembly costs of the battery pack. Despite these benefits, BMS wireless communications have high electromagnetic interference (EMI) susceptibility. As is fully discussed in Section 4, wireless communication will also increase the risk of cyberattacks on BMS communications. In [16], wireless BMSs and the related communication protocols based on Wi-Fi, Bluetooth, and Zigbee are reviewed in detail. The general architecture of the BMS is shown in Figure 3.

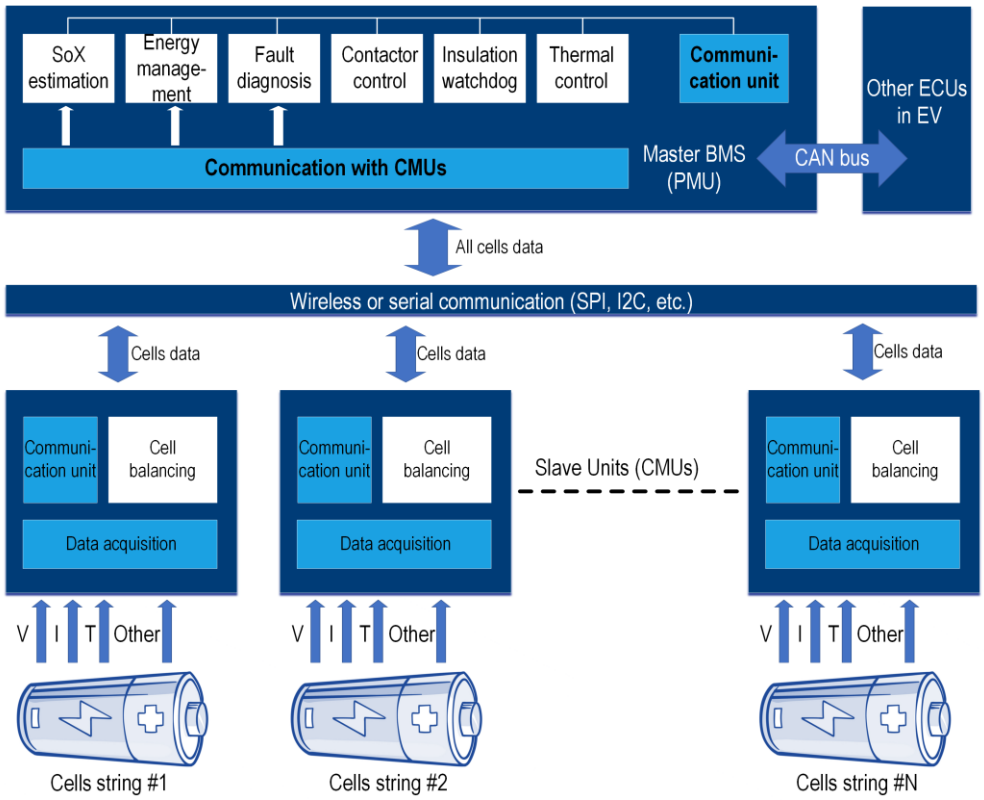

Figure 3. Typical architecture of a master–slave BMS.

The onboard BMS is usually equipped with microprocessors that have limited memory and computational power. This will place a limit on the achievable performance, since best-in-class algorithms may not be practicable. The limited BMS will compromise the battery pack and EV performance in terms of its safety, lifetime, driving range, etc. Adopting more powerful processors will result in increased BMS cost, which also increases the overall pack cost per EV and weakens the manufacturing economy at a large scale. Figure 4 shows the breakdown of the battery pack cost in a typical mid-size EV application [17]. As seen, the BMS currently constitutes about 8% of the overall pack cost and manufacturers tend not to pass beyond this range to maintain the overall EV affordability [4].

The limitations of the onboard BMS can be compensated by the CBMS. Thanks to powerful cloud computing servers, it is shown that the CBMS can support complicated physics-based models and AI/ML-based data-driven algorithms to achieve a superior level of performance in protection, monitoring, and control of the battery. Particularly, through the collection of large battery data and analyzing the history of the battery operation, the CBMS fulfills accurate prognosis and prediction of the system states that contribute to the enhanced safety of the pack. Nevertheless, the CBMS cannot fully supplant the onboard BMS due to safety reasons. Thus, the onboard BMS should be used to ensure the minimum safety requirements while the CBMS can be used alongside to compensate/enhance the core performance.

The conceptual framework of the CBMS is shown in Figure 5. As seen, the CBMS is used to complement the onboard BMS. The CBMS realization requires the establishment of different technologies: (1) high-performance cloud servers to host and run the required algorithms, store battery big data, and for data analysis; (2) an IoT platform to establish the two-way connection/communication between the physical BMS and the virtual BMS; (3) advanced modeling tools to establish physics-based battery digital twins to provide deeper insights to the condition and health of batteries; (4) a physical onboard BMS (generally a modular or master/slave BMS, but in principle, any architecture may be used depending on the required use cases) to fulfill the base functions related to sensing and

measurement, balancing control, etc. Different requirements of the CBMSs are reviewed in [4].

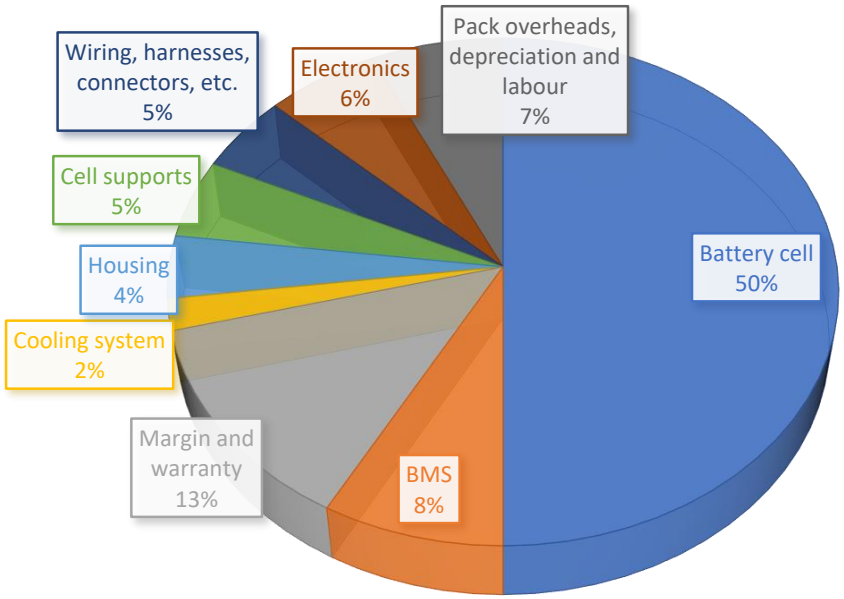

Figure 4. A breakdown of the battery pack costs for a mid-size EV application shows that BMS constitutes about 8% of the overall pack cost [17].

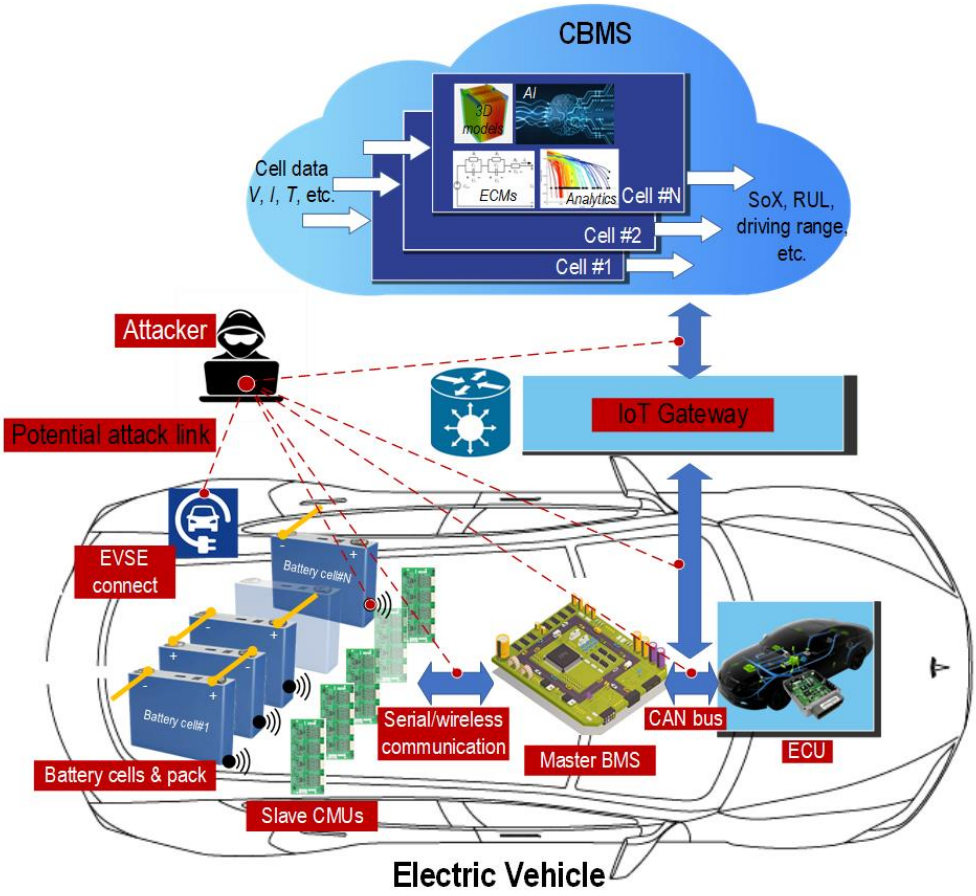

Figure 5. Concept diagram of the CBMS with potential attack surface.

Concerning the architecture, the CBMS consists of three main layers, namely, the hardware and connectivity layer, the analysis layer, and the service layer [4]. The hardware and connectivity is the lowest-level layer in the CBMS architecture and is responsible for edge-processing and collection of various sensory transaction data coming from the battery pack and the IoT platform. The transaction data may include, but are not limited to, battery current, cell voltages, cell temperatures, smoke sensor data, pressure, strain, etc. State data such as SoX information or processed data may also be transmitted to the CBMS to enable specific use cases. In practice, the types of data and transmission rate have to be optimized to reduce the burden on the communication and cloud. For example, instead of transmission of all raw battery data, more targeted data at regular intervals can be communicated to reduce the required bandwidth. The analysis layer is the middle layer and is responsible for storing, processing, and analyzing the battery data. Different battery data, such as transaction data, processed data, state data, and link data (metadata needed to link different models/algorithms/platforms in the service layer of the CBMS), should be stored here [4]. In addition, all the CBMS algorithms will be implemented in this layer. The uppermost layer is the service layer, which sometimes is also referred to as the application layer. It provides insight and visualizations of battery analytics results and also serves as an interface to connect to other platforms that require CBMS data. User interfaces (UIs) and application programming interfaces (APIs) will be implemented in this layer. There have been some extensions to the aforementioned core architecture. For instance, in some works, a separate database or storage layer is considered for storing different battery data, while some architectures also include a layer to address security/cybersecurity. A typical architecture of the CBMS is shown in Figure 6 [18].

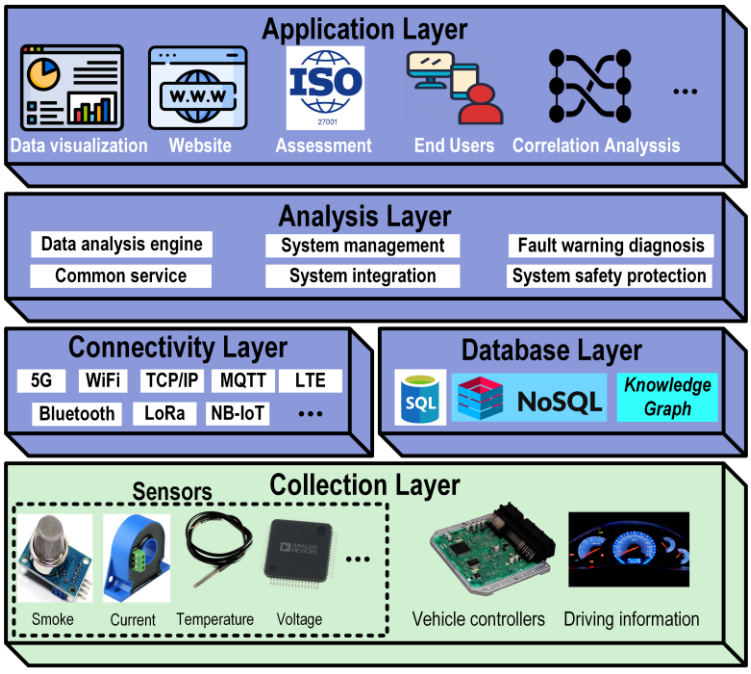

Figure 6. Functional architecture of a typical CBMS [18].

The exact architecture and functional model of the CBMS depend on the application area and specific use cases that should be implemented in the CBMS. The software and hardware architecture design should be flexible to adapt to a range of battery cell types, e.g., only with small fine-tuning of algorithms. Similarly, the choice of the vehicle-to-cloud (V2C) communication protocol depends on the specific requirements of use cases such as required bandwidth, latency, compression, data usage, and security protocols that they support. However, the protocol must support point-to-point communication with different message sizes and should achieve minimum communication delay [4]. The battery

pack of the EV is composed of hundreds to thousands of cells, and BMS measurements (including VIT) should usually be fulfilled at the cell level at a relatively high sampling rate. This means that a huge amount of data should be pushed toward the cloud. Thus, the CBMS IoT protocol must be able to handle the requirements related to bandwidth and delays. Reference [4] reviewed potential IoT protocols/technologies that can be applied to the CBMS context, where the potential of 5G-IoT is highlighted compared to other technologies, including LoRa, Wi-Fi, RabbitMQ, Message Queuing Telemetry Transport (MQTT), Modbus TCP/IP [19,20], and Hyper Text Transport Protocol (HTTP). Among these, MQTT has obtained increasing attention and is becoming the standard for IoT-based vehicular communications due to its simplicity, small code footprint, and relatively low latency. The MQTT protocol is based on the publish–subscribe messaging model, where the sender(s) and receiver(s) communicate through a central broker. MQTT often works on top of TCP/IP and can be enhanced with encryption techniques to ensure its security [20]. It is not the focus of this review to provide a detailed analysis of the security levels of different IoT protocols. On the other hand, this review tries to identify potential security scenarios and risks, which will then facilitate the security requirements of the IoT protocols.

Commercialized Examples of the CBMS Concept

Despite the fact that the CBMS is a recent concept, it has been implemented in industry to some extent. As an example, one can refer to the CBMS concept proposed by Bosch™ Mobility Solutions to supplement the onboard BMS in vehicles. The concept is referred to as "*Battery in the Cloud*" and contains a predictive cloud-based cooling algorithm that receives battery pack data, drive cycle, and charge station information through the IoT platform and controls the battery temperature to minimize degradation. Bosch's CBMS also includes an accurate algorithm for the prediction of the battery's remaining service life. The algorithm works based on the data collected from an entire fleet and not an individual EV. By taking into account different temperatures and driving conditions such as overly sporty driving styles, it is claimed that the CBMS can reduce the wear and tear on the battery by about 20% [21]. NXP® has also developed a new solution to connect the EV high-voltage BMS to the cloud to leverage the implementation of an AI-driven battery digital twin. The solution, which is named EVE-Ai™, provides more accurate predictions of SOC/SOH. The NXP's platform benefits multiple stakeholders. For instance, it provides efficient driver insights about driving range and recommendations about the optimum speeds to automakers and EV users. It also helps battery care centers to use in-depth battery data to speed up battery diagnostics and reduce downtime. The NXP's CBMS concept is based on two solution technologies, including NXP's S32K3-based reference design to enable ultra-accurate state predictions and NXP S32G vehicle networking processing solution for cloud-based automotive services [22]. Another example is the connected BMS proposed by Ricardo. The solution is developed for battery original equipment manufacturers (OEMs) to enable monitoring of the battery health through the application of ML to fleet data. The solution provides predictive maintenance so the early defects of the battery can be detected before they turn into serious faults [23]. Other use cases of the CBMS concept that have reached the market are reviewed in Table 2.

These examples clearly show the potential and trend for the marketability of the CBMSs. Despite these examples, the economy of CBMSs has been a debate point in academia and industry. BMS connectivity requires expensive infrastructure, high capital expenditure (CapEx), and large design effort in terms of communication, software, maintenance, and even its security, which is the main concern of this paper. The business cases should thus be carefully designed to create enough value and use cases that result in a faster return on investment (ROI). As an example, the economy of scale can be improved by considering shared CBMS services, e.g., to use CBMS services for a fleet of EVs rather than individual vehicles. Likewise, cloud implementation of simple algorithms such as cell balancing or basic protection functions might not bring added value compared to the onboard implementation, which already performs well.

Table 2. Commercial solutions that implement some of the CBMS use cases.

No.	Solution Name	Company	Description
1	Bosch™ Mobility Solutions	Bosch™	CBMS takes into account driving conditions such as driving style and driving environment (drive cycle) to adjust battery operation to maximize the battery lifetime. Battery tears and wear are deductible by about 20%.
2	EVE-Ai™	NXP	The CBMS is multifunctional and has AI-based SOC/SOH prediction capability. It offers recommendations in terms of remaining range and optimum driving speeds. Faster diagnostic and reduced downtime are achievable.
3	UBMC (Universal Battery Management Cloud)	Panasonic	The CBMS is based on a new AI-driven solution for accurate SOC prediction. The AI algorithm is trained with massive data accumulated at Panasonic during product development. It comes with an API to support fleet operators through the recommendation of service/replacement of batteries. It also contains a solution to provide the driving range in specific routes and a recommendation system to book the most convenient charging points [24].
4	Connected BMS	Ricardo	It offers advanced battery prognostics to reduce degradation and increase uptime. A +13% improvement in battery life is achievable [23].
5	CEBS (Cloud-enabled Battery Solution)	Replay	The CBMS is equipped with cell-level IoT sensors to transmit battery data toward an external gateway via mobile radio or WLAN to the cloud. The use cases are related to optimized battery charging [25].
6	Cloud-connected BMS	Fujitsu	It is based on a solution to grasp the condition of the shared batteries that will enable users to replace batteries (in swap stations) with peace of mind [26].
7	Batter Intelligence as a Service	Bamomas	The CBMS offers remote battery fleet monitoring, in-depth battery analytics, and predictive maintenance. It also offers a web application and an API to provide insights into the health and condition of batteries.
8	iBMS (intelligent BMS)	Udantech	It provides a cloud–terminal collaborative control to enhance the performance of the onboard BMS. It also supports SOC calibration and remote balancing.
9	COMSOL Server™, COMSOL Compiler™, and COMSOL API for use with Java®	COMSOL	Multiphysics models and battery digital twins produced in COMSOL can be used to update/calibrate the light-weighted models on the onboard BMS to maintain model fidelity over time

A broader concept that was recently introduced, known as vehicle-to-everything (V2E) or vehicle-to-X (V2X), further emphasizes the exchange of energy and data from/to vehicles. In V2X, X can be cloud (V2C), vehicle (V2V), grid (V2G), infrastructure (V2I), or pedestrian (V2P). Access points for V2X can be supported with a range of technologies, e.g., LTE-V2X and IEEE 802.11p are normally used for V2V and V2I, and IoT is used for V2C (similar to CBMS), while V2P is often implemented using Wi-Fi, Bluetooth, or cellular mobile communications [27]. All of this means that, in addition to BMS data, other information will be transmitted outside the vehicle, which further stresses the cybersecurity risk. Most importantly, these technologies are relatively new and their reliability is not fully proven. Similar to any new technology, it is important to analyze the cybersecurity of the CBMSs to ensure their reliability and safety. The review provided in the next section contributes to this analysis.

4. Cybersecurity of BMS

The probability of cyberattacks against EVs and CBMSs appears to be low but the risk is still high since such attacks, if successful, can lead to catastrophic incidents such as fire and the explosion of the battery pack. The EV batteries contain large amounts of energy and are thermally unstable systems. Cyberattacks against EV battery packs can thus lead to disastrous and life-threatening incidents. In addition to safety risks, cyberattacks might cause privacy and economic losses, e.g., by degrading/damaging the battery pack through overcharging and/or overdischarging, which will result in accelerated aging of the battery so the battery will die before its expected service time. Thus, it is critical to protect BMS against malicious attacks that can disrupt its proper performance in maintaining the pack's safety and performance. Cybersecurity must be ensured not only when the EV and battery are in use but also during charging or other modes of operation, such as the V2E concept, and even when the EV and battery are idle. Attacks can be launched internally at the system level through the in-vehicle CAN network, at the subsystem or component level through the BMS wireless communication network, externally through the IoT communications, or even through peripheral devices such as EVs onboard diagnostics (OBD) port [28]. There have been several examples of EV batteries becoming compromised. In the following, these incidents are briefly reviewed.

In 2016, a group of researchers demonstrated a successful hack of a Nissan Leaf, which enabled them to remotely drain the EV's battery pack. The hack was carried out by exploiting a vulnerability in Nissan's telematics system, which allowed the researchers to gain access to the BMS. The researchers were able to exploit the vulnerability by sending specially crafted packets of data to the EVs telematics system, which allowed them to take control of various systems in the car, including the climate control and the charging system of the BMS. By manipulating the heating system, the researchers were able to drain the car's battery, leaving it unable to start or drive [29]. Nissan responded to the hack by releasing a software patch for the affected vehicles and advising owners to update their cars as soon as possible [29]. In another case, a security specialist was able to hack 25 Tesla cars through their cellular connection and Wi-Fi related to their entertainment systems [30]. A similar attack was reported by the remote hijacking of a Cherokee Jeep being driven on the highway, which was launched via a cybersecurity breach in the control system [31].

Several cyberbreaches have also been reported regarding EVSEs. For instance, Kaspersky Lab reported a security breach in an EV charging application, which would let a remote attacker intrude into the charging system and tamper the system through the Wi-Fi connection [32]. A security breach was also reported in the EVlink chargers produced by Schneider Electric [33]. The breach would allow an attacker to bypass the authentication credentials, send malware, and deactivate the charging system.

Despite the continuous improvement of security systems, these examples show that hackers still can find new ways to infiltrate vehicle systems. This highlights the importance of robust cybersecurity measures to protect against such cyberthreats [34]. The cybersecurity of BESSs has been addressed in several works. Below, a brief review of the existing literature is provided.

4.1. Literature Review on BESS Cybersecurity

The operation of bidirectional EVSEs with V2G capability (also referred to as smart charging equipment [35]) should usually be scheduled and coordinated through effective communication channels between different stakeholders, including the EV owners, charge station operators, and grid operators [33]. V2G offers several advantages through different ancillary services such as peak shaving, demand side management, voltage/frequency stability support, reactive power compensation [35], etc. However, V2G has some challenging security issues [35]. 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 [36]. Several studies have thus analyzed the

cybersecurity of charging stations [37,38]. The authors of [33] 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 [33]. In [39], 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 [37], 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 [40,41], 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 [42]. With CCS, automated authentication and authorization can also be fulfilled through plug and charge (PnC) services [37]. A comparison of different charging protocols and their security features was presented in [37]. The impact of integrity attacks on the power electronics components of EV onboard chargers (OBCs) was examined in [43]. 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 [43].

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 [44]. In [45], 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 [46].

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

4.2. 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 [47,48]. Based on the cybersecurity literature, a secure CPS must satisfy three main requirements, related to confidentiality, integrity, and availability, also known as CIA [49]. The same CIA security requirements can be applied to the CBMS, as summarized in Figure 7.

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 8 depicts the CBMS cyberattacks classification depending on the CIA requirements attacked [44,50,51]. It should be noted that in some attack conditions, more than one CIA requirement might become compromised.

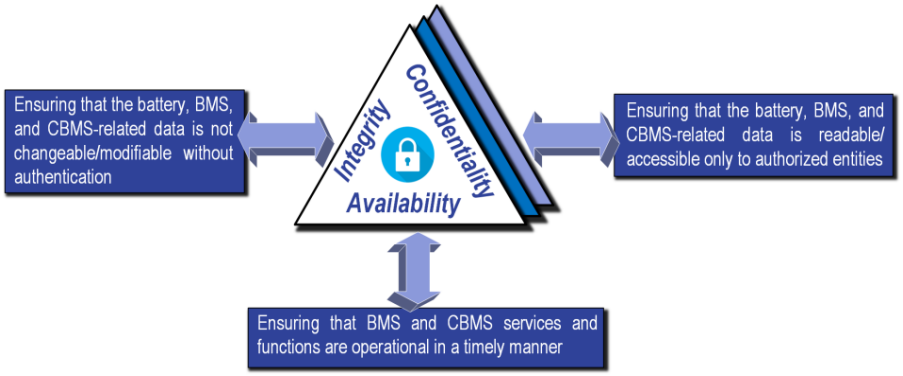

Figure 7. CIA requirements for CBMS cybersecurity.

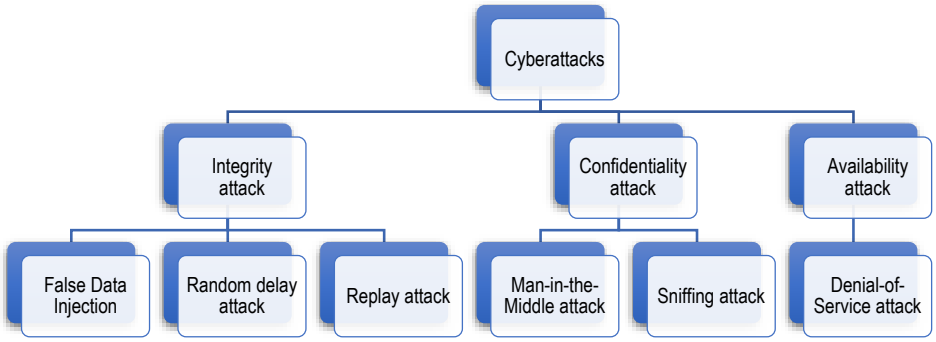

Figure 8. Classification of different potential cyberattacks against CBMS.

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 [44]. 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. [50] 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 9. 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 [50]. In Figure 9, activities refer to BMS functions or processes.

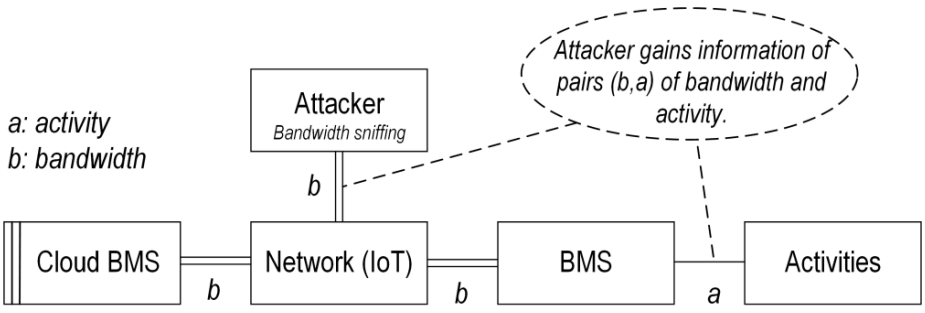

Figure 9. Illustration of the bandwidth sniffing attack.

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 [37]. 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 10a. Ref [50] 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 10b,c [50].

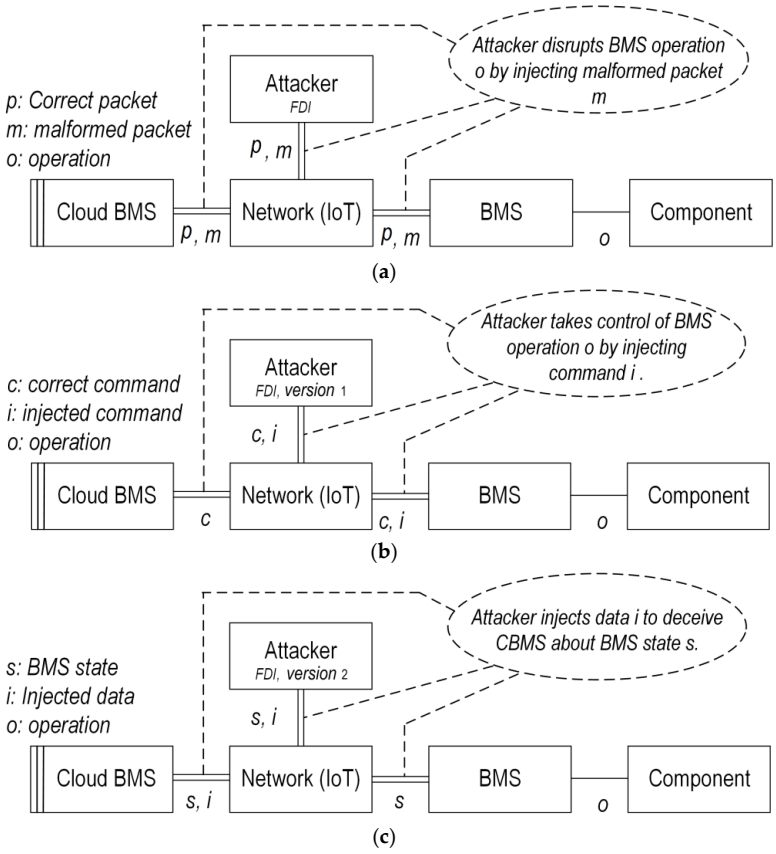

Figure 10. (**a**) Concept illustration of the FDI attack. (**b**) Variant 1 of the FDI attack. (**c**) Variant 2 of the FDI attack.

Likewise, Figure 11 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.

- Availability attacks: Refers to the denial-of-service (DoS), in which the attacker seeks to make the CBMS services unavailable to EVs [52]. 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.

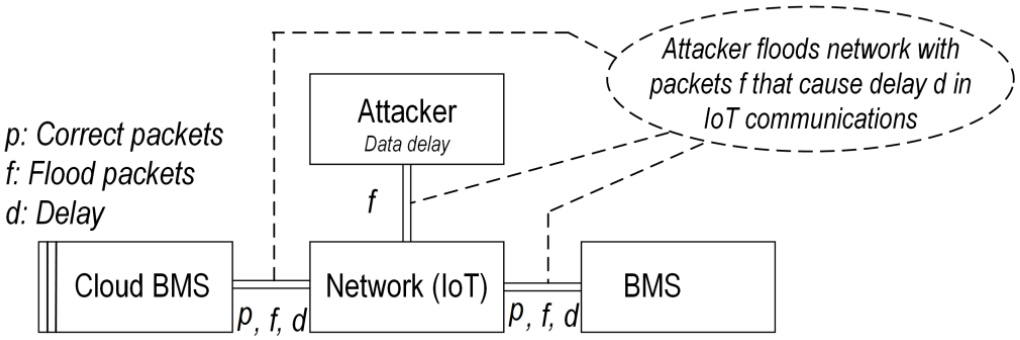

Figure 11. Illustration of the data delay attack.

In practice, loosely-secured CBMS-IoT networks are vulnerable to all types of attacks described before [37]. 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 [37]. In [51], 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 [35]. 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 [36]. 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 [35]. 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. In Section 6, 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 [19,20], CBMS interfaces to the cloud, etc. [53]. 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 [53]. 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 [54], 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 [55], 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. [28] 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.

4.3. 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 [28]. 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, [56] 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 [57]. 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 [29]. 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 [57]. 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 [58]. 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 [57], 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. [59]. Falsified BMS data such as wrong SoC and charge/power demand data can corrupt the performance of the power system, leading to overfrequency [60], underfrequency [61], voltage deviations [61,62], etc. [62]. In a recent study [63], 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.

4.4. CBMS 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 [64], giving a warning to the operator instead of shutting off the battery pack [65], 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 [66]. 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 [66]. Another approach for cyberattack detection is referred to as behavior-based detection [67]. 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 [67]. An example of ML-based attack detection is presented in [68], 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. [69] 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 [69]. A more detailed review of cyberattack detection techniques can be found in [70–72].

4.5. Methods for Enhancing the Cybersecurity of the BMS/CBMS

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 [55]. 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 [44], 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 [68]. 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 [52]. 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 12 [73].

The application of blockchain in the CBMS context has been explored in several research papers. In [74], 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 [32,75,76], 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. [77] 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 13.

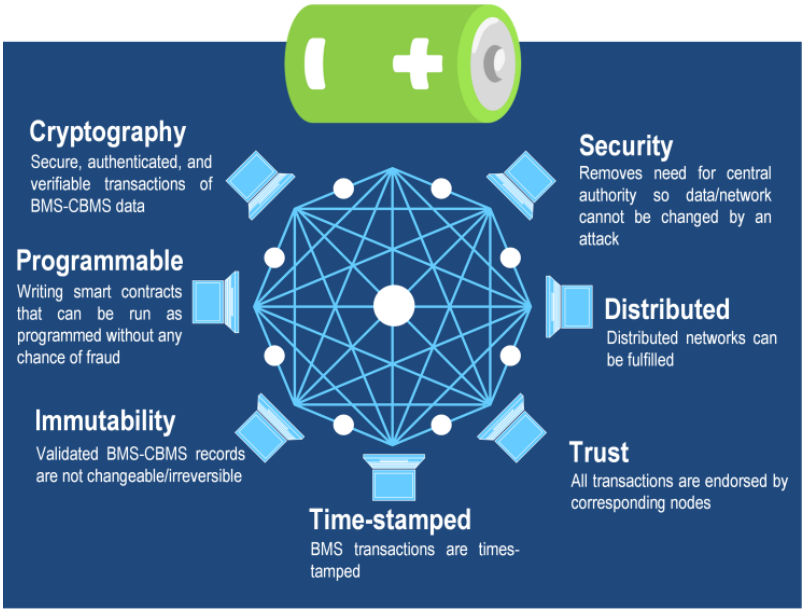

Figure 12. Main features of blockchain technology.

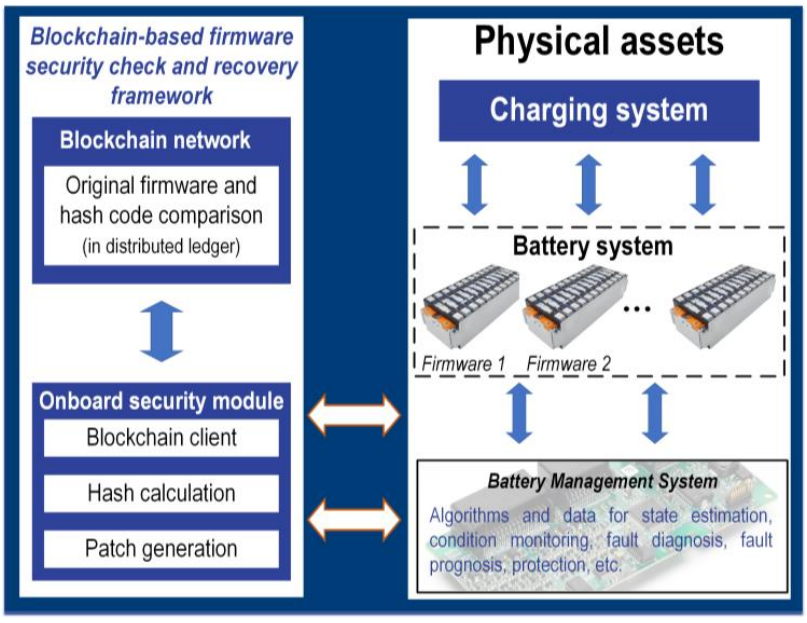

Figure 13. A typical architecture for blockchain-based firmware security enhancement [75].

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 [77]. 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 [54].

- *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. [78,79] 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 [80], 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 [30]. 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. [44] 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. [81] 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 [81], 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 [82]. The security of BMS source codes should also take into account reliable libraries throughout the source code [83].
- *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 [28]. 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 [84]. The basic architecture of an HSM is depicted in Figure 14. 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 [84]. 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 [84] 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.

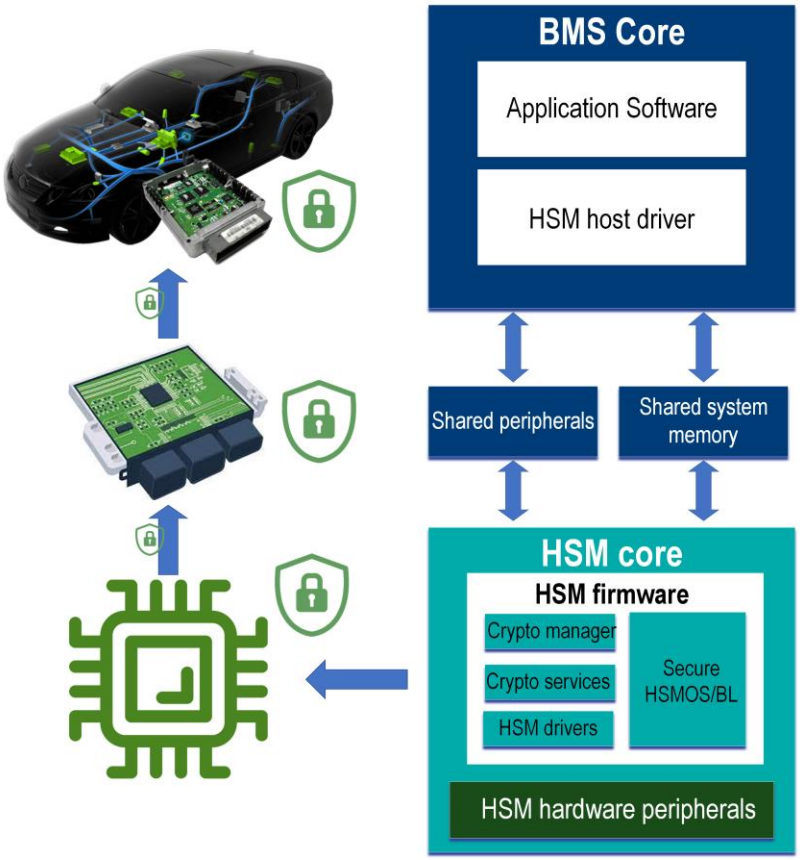

Figure 14. The architecture of the HSM (reproduced from [84]).

- *Encryption*: Encryption refers to the process of encoding BMS/CBMS software data/information to prevent unauthorized access and/or data alternation [85]. 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 [81]. 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 [86,87]. 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 [88]. 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. [81]. 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) [58]. 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. [89] 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* [90,91]: 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 [92]. Likewise, in the case of adopting the MQTT protocol for IoT communications, Ref. [81] 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. [81] 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 [28]. NREL recommends removing BMS unnecessary interfaces and external ports, adding tamper monitoring and resistance [93], adding secure bootloaders to BMS, removing hard-coded passwords, and certification of CBMS services with the Federal Risk and Authorization Management Program (FedRAMP) [40]. 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 [94]. Likewise, Refs. [28,44] 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 [28].

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 [95]. Table 3 provides a summary of key CBMS cybersecurity topics discussed in this section.

Table 3. 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 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.	▪ **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 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. ▪ **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.
Potential cyberattacks against CBMSs		**Attack Detection**	
Confidentiality	▪ **Sniffing (snooping) attack**: Attacker 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.	▪ **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.	
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.		
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.		

5. Existing Regulations and Standards

Several standards and regulations have been emplaced to ensure the safety and security of vehicles. For example, the ISO/SAE 21434 standard provides guidelines for the development of cybersecurity in road vehicles, while the UN Regulation No. 155 outlines specific requirements for cybersecurity management systems in vehicles. In addition, many countries have enacted legislation mandating the implementation of cybersecurity measures in vehicles, such as automotive cybersecurity guidelines released by the Japanese Information Technology Promotion Agency (IPA). These standards and regulations are crucial in ensuring that vehicles are secure. SAE J3061 is the first document that provides guidelines on cybersecurity of the electronic systems in vehicles [53].

Concerning vehicle BESSs, several standards highlight and take measures to address the safety risks, e.g., ISO 12405-part 4 [96] and IEC 62660-part 1 [97]. However, there is no existing standard that directly deals with the design requirements of CBMS (and even BMS) and the cybersecurity requirements. IEEE has released a draft recommended practice for the design of BMS physical and software interfaces but the security requirements have not been sufficiently addressed [98]. Nevertheless, several of the CBMS cybersecurity requirements can be derived by reviewing and analyzing the existing relevant standards related to the design of vehicular ECUs.

Table 4 lists the published standards/guidelines with relevance to the CBMS cybersecurity topic. The names of the standards, titles, and their relevance are described in different columns in Table 4.

Table 4. Standards/guidelines that can be related to the CBMS cybersecurity.

Standard/Policy/ Regulation	Year	Title	Relevance
SAE J3061 [99]	2016	Cybersecurity guidebook for cyber-physical vehicle systems.	• Provides cybersecurity requirements for vehicles. • Presents comprehensive cybersecurity process and management frameworks for vehicles. • Establishes the relationship between vehicle systems safety and cybersecurity. • Also details cybersecurity analysis, assurance, and test techniques applicable to vehicles.
ISO/IEC 27001 [100]	2022	Information security management systems.	• The standard sets requirements for the security of information assets and management/protection of sensitive data on cloud systems to assure CIA requirements. • It provides a robust framework for managing information security risks that could impact the security and safety of vehicles and CBMSs.
IEC62443 [101]	2009	Industrial communication networks—network and system security.	• An international series of standards that address the cybersecurity of automation and control systems. • Cover cybersecurity requirements for different stakeholders including system operators, service providers, and component/system manufacturers.
IEEE P2686 [102]	2019	Recommended practice for battery management systems in energy storage applications.	• Discusses design, installation, and configuration of BMSs for stationary applications. • Covers both hardware and software aspects such as requirements for wireless sensors and communications with external systems. • It does not cover the BMS in vehicular applications or BMS cybersecurity. • It applies to Li-ion, lead-acid, and flow batteries.

Table 4. *Cont.*

Standard/Policy/ Regulation	Year	Title	Relevance
ISO/SAE 21434 [103]	2021	Road vehicles—cybersecurity engineering.	• Specifies requirements for managing cybersecurity risks associated with the concept, system development, implementation, operation, and maintenance of electrical/electronic systems in road vehicles.
X.1373 [104]	2017	Secure software update capability for intelligent transportation system communication devices.	• Provides software security update program between the vehicle and a remote server (cloud). • Defines the process for security updates and content recommendations.
-	2022	Cybersecurity best practices for the safety of modern vehicles.	• Covers cybersecurity issues for all motor vehicles and their equipment (including software components).

SAEJ3061 draws a comparison between system safety and system cybersecurity. The scope of cybersecurity is deemed broader than safety, i.e., EV components that are safety-critical are also cybersecurity-critical, but not vice-versa. Equivalent to ASILs that address safety, SAE 21434 describes Automotive Cybersecurity Integration Levels (ACILs) to quantify the requirements for EV cybersecurity. The same concept can be applied to define ACILs for different systems, components, processes, and algorithms of the CBMSs. As recommended by SAEJ3061, cybersecurity must be built into the feature rather than adding it at the end stages of the development phase. ISO 21434 adds that cybersecurity should be addressed throughout the lifecycle from product development toward the end-of-life (EoL). This is important for particular use cases, e.g., when the battery, BMS, or CBMS should be moved to the second-life, recycled, etc. Thus, determining how to ensure cybersecurity when moving CBMS (battery data, usage history, critical information, etc.) to the next lifecycle stage is important to address. Cybersecurity should thus be guaranteed throughout the whole lifecycle and supply chain of battery and CBMS. For instance, manipulation of the data at the production and testing phase can lead to defective design processes for CBMS, e.g., the algorithms might be trained and tested based on incorrect data, which can cause a failure during actual operation. The cybersecurity lifecycle framework is depicted in Figure 15.

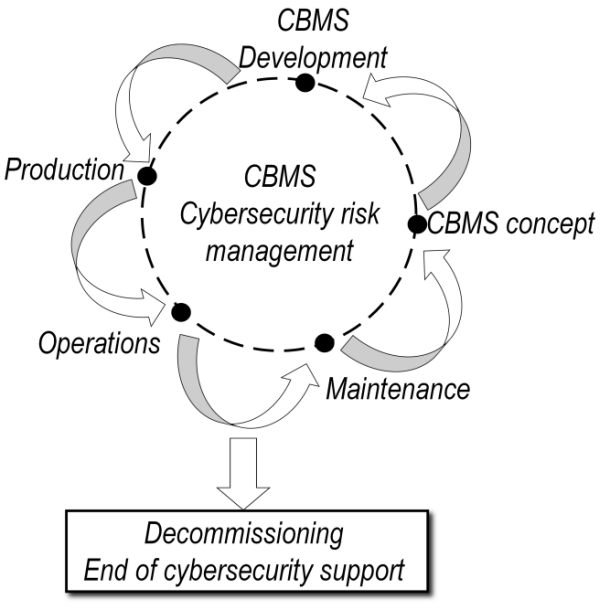

Figure 15. Cybersecurity lifecycle for CBMS development, production, operation, and maintenance.

Similar to the Hazard Analysis and Risk Assessment (HARA) described in ISO26262, SAE J3061 and ISO/SAE 21434:2021 propose a framework for Threat Analysis and Risk Assessment (TARA) [83]. Several analysis tools are also suggested to support TARA, including techniques and templates for threat scenario identification, impact rating, attack path analysis, attack feasibility rating, etc. Nevertheless, there is a gap regarding providing recommendations on the specifics of the EV components, including the CBMSs. In [83], the Framework for Analysis, Comparison, and Test of Standards (FACTS) was proposed by taking into account key CBMS stakeholders including battery producers, BMS producers, OEMs and EV manufacturers, battery test facilities, battery suppliers, consumers, etc. The FACTS approach is a four-step tool comprising stakeholder analysis, technical analysis, comparison of standards concerning the stated intrusion detection and mitigation mechanisms, and, finally, test and validation [83].

Standards have also proposed different tools for CBMS cybersecurity testing, for example, through performing automated software testing approaches such as data fuzz testing. Power hardware-in-the-loop (PHiL) can assess the CBMS capability to integrate, interact, and transfer data with the rest of the vehicle nodes. PHiL can also be used to assess the likelihood of a hardware trojan. Model-in-the-loop (MiL) can be used to test the CBMS algorithms and controllers in an emulated controlled environment while executing any possible transients that may occur due to the occurrence of cyberattacks [83]. Likewise, SAE J3061 suggests various cybersecurity testing tools including static code analyzers, dynamic code analyzers, network traffic analyzers, fuzz testers, encryption crackers, hardware debuggers, network stress testers, etc.

6. Potential Future Research Domains

BMS cybersecurity is a trending topic but there are still many gaps that have to be filled. According to the review, the potential future research domains are identified and outlined as follows:

- *TARA analysis and definition of ACILs*: A detailed TARA analysis needs to be fulfilled to understand different cyberthreats and their influence on the CBMS performances and the associated risks to EVs' functional safety. Such analysis will further help to quantify the ACILs required for CBMS cybersecurity design procedures, as suggested in SAE J3061. This review reviewed and addressed the potential threats to some extent. However, their link to ACILs is yet to be established in future works. New BMS architectures and topologies are being proposed and it is important to identify new vulnerabilities associated with them. For example, the effect of EMI attacks on wireless BMSs can be further explored.
- *Cybersecurity analysis, test, and validation platforms*: The cybersecurity of BMS is a recent topic and there is still a lack of modeling and simulation tools that can be used to analyze, test, and validate cybersecurity designs. As an example of such cybersecurity test setups, one can refer to the open-source platform named CEE developed by NREL, which is capable of emulating both physical land network aspects (including OCPP or Open Charge Point Protocol) of EVSEs [36]. The platform was successfully used to emulate different attack scenarios such as DOS and MitM attacks. Further research is required to develop more flexible platforms to enable the assessment of a broader range of use cases.
- *Algorithm design*: New efficient algorithms should be designed to reinforce CBMS cybersecurity. This involves the design of secure and resilient algorithms that are robust against cyberattacks, such as manipulated data. Likewise, detection algorithms should be designed and integrated into the CBMS to enable the detection of cyberattacks. Discussions regarding how the CBMS should respond to such attacks (in terms of battery control and prioritization of signals from the cloud) also need further exploration. The algorithm design should also take into account the possibility of system faults and preferably be capable of distinguishing between attack conditions and failure conditions (e.g., failures in sensors, etc.).

- *Cybersecurity in second life*: CBMS cybersecurity should further be explored in different lifecycle stages, including when moving EV batteries from first-life to second-life. In this context, future work can focus, for example, on how to pass on battery-related data from one stage of life to another in a secure manner. Research should be fulfilled to determine which data, when, and how it should be transferred while ensuring the cybersecurity requirements.

- *A systematic review of individual topics*: This paper is a scoping review where various topics related to CBMS cybersecurity are discussed. In the future, full systematic reviews can be carried out to analyze each aspect in more depth. For instance, some topics such as cyberattack detection methods, etc., require a dedicated review study.
- *Standardization:* The standards review fulfilled in Section 5 showed that no standards exist to address the design requirements of the BMS, CBMS, and their cybersecurity requirements. However, as reviewed, many useful tools and frameworks are proposed for automotive cybersecurity, including SAE J3061 and ISO 21434. Such tools can be used to further analyze cybersecurity in the CBMS context and develop new requirements and/or tailor the existing requirements for the DFC.
- *Artificial Intelligence for BMS Cybersecurity*: AI can be used to process vast amounts of battery data to establish baseline behavioral patterns and use them to continuously monitor the CBMS concerning cyberattacks. AI can also leverage threat intelligence feeds, security databases, and historical cyberattack data to identify potential vulnerabilities and predict emerging threats against the CBMS. Last, but not least, AI-powered incident response systems can be used to automate the identification, containment, and remediation of cyberattacks, minimizing the impacts on the CBMS, battery, and EV/grid operations.
- *Implementation:* Research can also be focused to address the implementation challenges of the CBMSs, e.g., establishment of proper communication tools and protocols (with sufficient bandwidth and acceptable data transmission delay) to support a sustainable, smooth, and secure two-way transmission of data between physical and digital BMSs. Likewise, the design of CBMS architecture can be enhanced to address the flexibility, modularity, scalability, and cybersecurity of the cloud platform.

This work is accomplished as part of the DeepBMS project which is funded under EU's Horizon Europe Framework. The project is exploring, among other things, the implementation of a CBMS concept to enable advanced functionalities. More results on some of the previous items are expected to be disseminated in the future.

7. Conclusions

In the form of a scoping review, this paper analyzes various security aspects relevant to the CBMSs. In the review, a detailed analysis of onboard BMSs and CBMSs is carried out. The architecture, requirements, and challenges of each technology are reviewed. It is concluded that the presence of the onboard BMS is critical to ensure EVs' functional safety and it is suggested to use CBMS for complementing the BMS core performance. Likewise, the review of commercial examples of CBMSs is presented, which shows the great potential for the marketability of this technology. Bosch^{TM}, NXP, and Panasonic are among the popular companies that have implemented some use cases of the CBMSs. Various topics related to the cybersecurity of CBMSs are explored. Firstly, potential attack types and scenarios are reviewed. They are mainly classified as confidentiality attacks, integrity attacks, and availability attacks. The potential attack paths are analyzed afterward. The attack path analysis shows several vulnerabilities, including the in-vehicle communications such as CAN bus, ports, and interfaces such as OBD-II, and extra-vehicle communications such as interfaces of IoT gateway, cloud, and underlying protocols. A short review of possible cyberattack impacts is also fulfilled, including denial-of-charging, depletion of the battery pack, accelerated aging of batteries, and thermal runway in more severe scenarios. The paper also contributes to the review of cyberattack detection algorithms and possible countermeasures that can be considered to improve CBMS cybersecurity. As for the

latter, several methods such as using blockchain, designing resilient algorithms, enforcing encryption and authentication mechanisms, etc., are discussed in detail. The standard landscape review is also fulfilled, which clearly shows the lack of proper standardization regarding CBMS cybersecurity design. However, existing standards such as SAE J3061 and ISO 21434 provide useful guidelines to address this topic, e.g., through suggesting cybersecurity test methods, TARA analysis, and ACIL assignment. Finally, the paper ends with a list of potential future research domains in the field of BMS cybersecurity.

Author Contributions: Conceptualization, F.N. and E.S.; methodology, F.N., P.G.L., Z.K., M.M.A. and E.S.; formal analysis, F.N. and Z.K.; investigation, F.N., Z.K., P.G.L., M.M.A. and E.S.; resources, F.N. and E.S.; writing—original draft preparation, F.N., E.S. and Z.K.; writing—review and editing, E.S., P.G.L., Z.K. and M.M.A.; visualization, F.N.; supervision, E.S.; project administration, F.N. and E.S.; funding acquisition, F.N. and E.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is fulfilled within the framework of the DeepBMS project which has received funding from the European Union's Horizon Europe Program under Marie Skłodowska-Curie Actions with grant agreement No. 101064083. We are grateful to the Poul Due Jensen Foundation, which has supported the establishment of the Center for Digital Twin Technology at Aarhus University.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing does not apply to this article.

Acknowledgments: This work was fulfilled within the framework of the DeepBMS project which received funding from the European Union's Horizon Europe Program under Marie Skłodowska-Curie Actions with grant agreement No. 101064083. We are grateful to the Poul Due Jensen Foundation, which has supported the establishment of the Center for Digital Twin Technology at Aarhus University.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

Acronym	Definition
ACIL	Automotive Cybersecurity Integration Level
AI	Artificial Intelligence
ANN	Artificial Neural Network
ASIL	Automotive Safety Integrated Level
BaaS	Blockchain-as-a-Service
BESS	Battery Energy Storage System
BMS	Battery Management System
CAN	Controller Area Network
CBMS	Cloud BMS
CCS	Combined Charging System
CEBS	Cloud-Enabled Battery Solution
CIA	Confidentiality, Integrity, Availability
CMU	Cell Monitoring Unit
CPS	Cyber-Physical System
DDoS	Distributed Denial-of-Service
DFC	Design-for-Cybersecurity
DoS	Denial-of-Service
E2E	End-to-End
ECM	Equivalent Circuit Model
ECU	Electronic Control Unit
EMI	Electromagnetic Interference
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FDI	False Data Injection
FPGA	Field Programmable Gate Array

FSDD	False Sensor Data Detection
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HTTP	Hyper Text Transport Protocol
IoT	Internet of Things
Li-on	Lithium-ion
MitM	Man-in-the-Middle
ML	Machine Learning
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MQTT	Message Queuing Telemetry Transport
OBC	Onboard Charger
OBD	Onboard Diagnostics
OEM	Original Equipment Manufacturer
PMU	Pack Monitoring Unit
SoC	State-of-Charge
SoH	State-of-Health
SoP	State-of-Power
SoX	State-of-X
TARA	Threat Analysis and Risk Assessment
TLS	Transport Layer Security
TRL	Technology Readiness Level
UBMC	Universal Battery Management Cloud
V2C	Vehicle-to-Cloud
V2E	Vehicle-to-Everything
V2G	Vehicle-to-Grid
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VIT	Voltage, Current, Temperature
WPTM	Wireless Power Transfer Module

References

1. Zhou, L.; Lai, X.; Li, B.; Yao, Y.; Yuan, M.; Weng, J.; Zheng, Y. State Estimation Models of Lithium-Ion Batteries for Battery Management System: Status, Challenges, and Future Trends. *Batteries* **2023**, *9*, 131. [CrossRef]
2. Habib, A.A.; Hasan, M.K.; Issa, G.F.; Singh, D.; Islam, S.; Ghazal, T.M. Lithium-Ion Battery Management System for Electric Vehicles: Constraints, Challenges, and Recommendations. *Batteries* **2023**, *9*, 152. [CrossRef]
3. Gandoman, F.H.; El-Shahat, A.; Alaas, Z.M.; Ali, Z.M.; Berecibar, M.; Abdel Aleem, S.H. Understanding Voltage Behavior of Lithium-Ion Batteries in Electric Vehicles Applications. *Batteries* **2022**, *8*, 130. [CrossRef]
4. Naseri, F.; Gil, S.; Barbu, C.; Cetkin, E.; Yarimca, G.; Jensen, A.; Larsen, P.; Gomes, C. Digital twin of electric vehicle battery systems: Comprehensive review of the use cases, requirements, and platforms. *Renew. Sustain. Energy Rev.* **2023**, *179*, 113280. [CrossRef]
5. Naseri, F.; Barbu, C.; Sarikurt, T. Optimal sizing of hybrid high-energy/high-power battery energy storage systems to improve battery cycle life and charging power in electric vehicle applications. *J. Energy Storage* **2022**, *55*, 105768. [CrossRef]
6. Naseri, F.; Schaltz, E.; Stroe, D.-I.; Gismero, A.; Farjah, E. An enhanced equivalent circuit model with real-time parameter identification for battery state-of-charge estimation. *IEEE Trans. Ind. Electron.* **2021**, *69*, 3743–3751. [CrossRef]
7. Naseri, F.; Karimi, S.; Farjah, E.; Schaltz, E. Supercapacitor management system: A comprehensive review of modeling, estimation, balancing, and protection techniques. *Renew. Sustain. Energy Rev.* **2022**, *155*, 111913. [CrossRef]
8. Xing, Y.; Ma, E.W.; Tsui, K.L.; Pecht, M. Battery management systems in electric and hybrid vehicles. *Energies* **2011**, *4*, 1840–1857. [CrossRef]
9. Wang, Y.; Tian, J.; Sun, Z.; Wang, L.; Xu, R.; Li, M.; Chen, Z. A comprehensive review of battery modeling and state estimation approaches for advanced battery management systems. *Renew. Sustain. Energy Rev.* **2020**, *131*, 110015. [CrossRef]
10. Crawford, A.J.; Choi, D.; Balducci, P.J.; Subramanian, V.R.; Viswanathan, V.V. Lithium-ion battery physics and statistics-based state of health model. *J. Power Sources* **2021**, *501*, 230032. [CrossRef]
11. Li, W.; Rentemeister, M.; Badeda, J.; Jöst, D.; Schulte, D.; Sauer, D.U. Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation. *J. Energy Storage* **2020**, *30*, 101557. [CrossRef]
12. ISO 26262-1:2018. Road Vehicles—Functional Safety. 2018. Available online: https://www.iso.org/standard/68383.html (accessed on 21 May 2023).

13. Xu, J.; Li, S.; Mi, C.; Chen, Z.; Cao, B. SOC based battery cell balancing with a novel topology and reduced component count. *Energies* **2013**, *6*, 2726–2740. [CrossRef]
14. Gocmen, S.; Cetkin, E. Experimental investigation of air cooling with/out tab cooling in cell and module levels for thermal uniformity in battery packs. *ASME J. Heat Mass Transf.* **2023**, *145*, 022903. [CrossRef]
15. Piao, C.H.; Cong, T. Study on isolation monitoring of high-voltage battery system. *Appl. Mech. Mater.* **2011**, *44*, 571–575. [CrossRef]
16. Samanta, A.; Williamson, S.S. A survey of wireless battery management system: Topology, emerging trends, and challenges. *Electronics* **2021**, *10*, 2193. [CrossRef]
17. Schneider, G.; Maier, H.; Häcker, J.; Siegele, S. Electricity storage with a solid bed High Temperature Thermal Energy Storage system (HTTES)—A methodical approach to improve the pumped thermal grid storage concept. In Proceedings of the 14th International Renewable Energy Storage Conference 2020 (IRES 2020), Düsseldorf, Germany, 10–12 March 2020; pp. 26–33.
18. Yang, S.; Zhang, Z.; Cao, R.; Wang, M.; Cheng, H.; Zhang, L.; Jiang, Y.; Li, Y.; Chen, B.; Ling, H. Implementation for a cloud battery management system based on the CHAIN framework. *Energy AI* **2021**, *5*, 100088. [CrossRef]
19. 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. [CrossRef]
20. 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. [CrossRef]
21. McMahan, S. Bosch Cloud-Based Battery Management System Extends EV Battery Life. Available online: https://eepower.com/news/bosch-cloud-based-battery-management-extends-ev-battery-service-life/# (accessed on 21 May 2023).
22. Semiconductors, N. AI-Powered Cloud-Connected Battery Management System for Electric Vehicles. NXP Semiconductors. Available online: https://www.nxp.com/company/about-nxp/ai-powered-cloud-connected-battery-management-system-for-electric-vehicles:NW-NXP-AI-POWERED-CLOUD-CONNECTED-BATTERY (accessed on 21 May 2023).
23. Ricardo. Connected Battery Management System. Available online: https://www.ricardo.com/en/services/technical-consulting/software-development-and-applications/connected-battery-management-system (accessed on 21 May 2023).
24. Panasonic. Panasonic Announces UBMC Service—A Cloud-Based Battery Management Service to Ascertain Battery State in Electric Mobility Vehicles. Available online: https://news.panasonic.com/global/press/en201210-1 (accessed on 21 May 2023).
25. REPLY. Cloud-Enabled Battery Solution—CEBS. Available online: https://www.reply.com/en/automotive-and-manufacturing/cloud-enabled-battery-solution-cebs (accessed on 21 May 2023).
26. Tanizawa, T.; Suzumiya, T.; Ikeda, K. Cloud-connected battery management system supporting e-mobility. *Fujitsu Sci. Tech. J.* **2015**, *51*, 27–35.
27. Möller, D.P.; Haas, R.E. *Guide to Automotive Connectivity and Cybersecurity*; Springer: Berlin/Heidelberg, Germany, 2019.
28. Madeline, C.; Richard, S. Cybersecurity of Battery Management Systems. In *Readout: Horiba Technical Reports*; HORIBA: Singapore, 2019; pp. 82–89.
29. Eiza, M.H.; Ni, Q. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Veh. Technol. Mag.* **2017**, *12*, 45–51. [CrossRef]
30. 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.
31. Greenberg, A. Hackers remotely kill a jeep on the highway. *Wired* **2015**, *7*, 21–22.
32. Ochoa, J. *Security-Enhanced Cyber-Physical Battery Management System Using Blockchain and Security Hardening Technology*; Texas A&M University: Kingsville, TX, USA, 2020.
33. Gumrukcu, E.; Arsalan, A.; Muriithi, G.; Joglekar, C.; Aboulebdeh, A.; Zehir, M.A.; Papari, B.; Monti, A. Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Cappadocia, Turkey, 14–17 June 2022; pp. 506–511.
34. Hong, J. Cyber security issues in connected vehicle of intelligent transport system. *Indian J. Sci. Technol.* **2016**, *9*, 96027. [CrossRef]
35. Bhusal, N.; Gautam, M.; Benidris, M. Cybersecurity of electric vehicle smart charging management systems. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Virtual Event, 11–14 April 2021; pp. 1–6.
36. 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.
37. 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.
38. Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE Access* **2020**, *8*, 214434–214453. [CrossRef]
39. 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.
40. Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. *Energies* **2022**, *15*, 3931. [CrossRef]
41. 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. [CrossRef]

42. 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).
43. Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of onboard charging systems for electric vehicles—Review, challenges and countermeasures. *IEEE Access* **2020**, *8*, 226982–226998. [CrossRef]
44. Kharlamova, N.; Hashemi, S.; Træholt, C. Data-driven approaches for cyber defense of battery energy storage systems. *Energy AI* **2021**, *5*, 100095. [CrossRef]
45. 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.
46. Maheshwari, P.U.; Bhargavi, S.; Umarani, S. Advancements in Cyber Security for Autonomous Vehicles. *Int. J. Wirel. Netw. Secur.* **2021**, *7*, 33–40.
47. 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.
48. 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).
49. 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. [CrossRef]
50. 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.
51. 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.
52. 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. [CrossRef]
53. Yang, S.; Liu, X.; Li, S.; Zhang, C. *Advanced Battery Management System for Electric Vehicles*; Springer Nature: Berlin/Heidelberg, Germany, 2022.
54. 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. [CrossRef]
55. 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. [CrossRef]
56. Rohde, K.W. *Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid*; Idaho National Lab. (INL): Idaho Falls, ID, USA, 2019.
57. Sripad, S.; Kulandaivel, S.; Pande, V.; Sekar, V.; Viswanathan, V. Vulnerabilities of electric vehicle battery packs to cyberattacks. *arXiv* **2017**, arXiv:1711.04822.
58. Hodge, C.; Hauck, K.; Gupta, S.; Bennett, J.C. *Vehicle Cybersecurity Threats and Mitigation Approaches*; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2019.
59. 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.
60. 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. [CrossRef]
61. 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.
62. 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.
63. 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. [CrossRef]
64. 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.
65. Xie, J.; Chen, J.; Li, L.; Chen, Y. Advanced Battery Early Warning and Monitoring System. U.S. Patent US9177466B2, 3 November 2015.
66. 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. [CrossRef]
67. 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.
68. 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.

69. Dey, S.; Khanra, M. Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging. *IEEE Trans. Ind. Electron.* **2020**, *68*, 478–487. [CrossRef]
70. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
71. 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. [CrossRef]
72. 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. [CrossRef]
73. 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. [CrossRef]
74. 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.
75. 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.
76. 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. [CrossRef]
77. 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.
78. 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. [CrossRef]
79. 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. [CrossRef]
80. 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. [CrossRef]
81. 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.
82. 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).
83. 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.
84. Bierbaum, D.; Stampa, R. Smart Synthesis of Cybersecurity and Functional Safety. *ATZelectron. Worldw.* **2021**, *16*, 8–11. [CrossRef]
85. 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. [CrossRef]
86. 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.
87. 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.
88. 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.
89. 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.
90. ElaadNL. *Security Architecture for Electric Vehicle Charging Infrastructure, Version 1.0*; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
91. ElaadNL. *Security Architecture for Electric Vehicle Charging Infrastructure, Version 2.0*; European Network for Cyber Security: Den Haag, The Netherlands, 2019.
92. 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.
93. 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.

94. 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.
95. Alcaraz, C.; Lopez, J. Digital twin: A comprehensive survey of security threats. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1475–1503. [CrossRef]
96. ISO 12405-4:2018. Electrically Propelled Road Vehicles—Test Specification for Lithium-Ion Traction Battery Packs and Systems—Part 4: Performance Testing. 2018. Available online: https://www.iso.org/standard/71407.html (accessed on 21 May 2023).
97. IEC 62660-1:2018. Secondary Lithium-Ion Cells for the Propulsion of Electric Road Vehicles—Part 1: Performance Testing. 2018. Available online: https://webstore.iec.ch/publication/28965 (accessed on 21 May 2023).
98. Rosewater, D.M. *IEEE Draft Battery Management System (BMS) Recommended Practice*; Sandia National Lab. (SNL-NM): Albuquerque, NM, USA, 2020.
99. J3061_201601. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. 2016. Available online: https://www.sae.org/standards/content/j3061_201601/ (accessed on 21 May 2023).
100. ISO/IEC 27001. Information Security Management Systems. 2022. Available online: https://www.iso.org/standard/27001 (accessed on 21 May 2023).
101. IEC 62443-4-2:2019. Security for Industrial Automation and Control Systems—Part 4-2: Technical Security Requirements for IACS Components. 2019. Available online: https://www.iecee.org/certification/iec-standards/iec-62443-4-22019-34421 (accessed on 21 May 2023).
102. P2686. Recommended Practice for Battery Management Systems in Energy Storage Applications. 2018. Available online: https://standards.ieee.org/ieee/2686/7394/ (accessed on 21 May 2023).
103. ISO/SAE 21434:2021. Road Vehicles—Cybersecurity Engineering. 2021. Available online: https://www.iso.org/standard/70918.html (accessed on 21 May 2023).
104. X.1373. Vehicle-to-Infrastructure: Secure Software Update. 2017. Available online: https://www.itu.int/rec/T-REC-X.1373-201703-I/en (accessed on 21 May 2023).