IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 December 2024, accepted 4 February 2025, date of publication 18 February 2025, date of current version 3 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3543249

SURVEY

Battery Management System: Threat Modeling, Vulnerability Analysis, and Cybersecurity Strategy

SHRAVAN MURLIDHARAN, VARSHA RAVULAKOLE, JYOTHI KARNATI, AND HAFIZ MALIK, (Senior Member, IEEE)

Information Systems, Security, and Forensics Laboratory, University of Michigan-Dearborn, Dearborn, MI 48128, USA

Corresponding author: Hafiz Malik (hafiz@umich.edu)

This work was supported in part by the National Science Foundation (NSF) under Award # 2414729, Award 2214830, and Award 2035770.

ABSTRACT The Battery Management System (BMS) plays a crucial role in modern energy storage technologies, ensuring battery safety, performance, and longevity. However, as the BMS becomes more sophisticated and interconnected, it faces increasing cybersecurity challenges that can lead to catastrophic failures and safety hazards. This paper provides a comprehensive overview of cyberattacks targeting both traditional and wireless BMS. It explores various attack vectors, including malware injection, electromagnetic interference (EMI), temperature sensing manipulation, sensor malfunctioning and fault injection, and jamming attacks on modern BMS. Through threat modeling and vulnerability analysis, this paper examines the potential impacts on BMS functionality, safety, and performance. We highlight vulnerabilities associated with different BMS architectures and components, emphasizing the need for robust cybersecurity measures to protect against emerging threats. Cybersecurity measures are essential to protect the system from potential threats that could trigger false alarms, cause malfunctions, or lead to dangerous failures. Unauthorized access or tampering with the BMS can disrupt its fault response mechanisms, jeopardizing system performance and associated resources. Key cybersecurity strategies include intrusion detection systems (IDS), crypto-based authentication, secure firmware updates, and hardware-based security mechanisms such as trusted platform modules (TPMs). These measures strengthen BMS resilience by preventing unauthorized access and ensuring data integrity. Our findings are essential for mitigating risks in various sectors, including electric vehicles (EVs), renewable energy, and grid storage. They underscore the importance of ongoing research and development of adaptive security strategies to safeguard BMS against evolving cyber threats. Additionally, we propose a trust mechanism that secures the connection between input sensors and the BMS, ensuring the reliability and safety of battery-powered systems across various industries.

INDEX TERMS Battery management systems (BMS), cybersecurity, electric vehicles (EVs), fault detection, malware attacks, electromagnetic interference (EMI), temperature sensing, wireless battery management systems (wBMS), jamming attacks, sensor manipulation attacks.

I. INTRODUCTION

The battery management system (BMS) plays a pivotal role in battery pack performance optimization, safety, and longevity across a wide range of applications, from portable consumer electronics like laptops and smartphones to EVs and large-scale grid energy storage systems. Conceived initially to mitigate fundamental risks like overcharging, high temperatures, and deep discharge, BMS has evolved into a sophisticated and intelligent system that acts as the central nervous system for battery-powered systems. In EVs, for instance, a BMS plays a critical role in managing the complex battery operation that powers cyber-physical systems and smart infrastructure, including EVs, robots, unmanned aerial

The associate editor coordinating the review of this manuscript and approving it for publication was Fabio Massaro.

vehicles (UAVs), etc. However, its responsibilities go far beyond ensuring basic safety parameters. Modern BMS continuously monitors and optimizes the health of individual battery cells, including real-time tracking of various cell parameters such as voltage, State of Charge (SOC), State of Health (SOH), and precise temperature. Such comprehensive monitoring not only helps prevent potential failures that could damage the battery pack or even cause safety hazards, but it also helps maximize energy efficiency and extend the operational lifespan of the battery [1].

The market for BMS is experiencing rapid growth in the automotive industry [2], stationary energy storage, and consumer electronics. Two main factors primarily drive it: (i) the increasing adoption of EVs and (ii) the expanding renewable energy sector. Tier-I auto-suppliers, including Bosch [3], Denso [4], and Continental [5] have developed state-of-the-art BMS for various industrial applications. The global BMS market is projected to reach USD 24.7 billion by 2030, growing at a CAGR of 18.3 percent. The automotive sector leads, accounting for over 55 percent of the market share, driven by increasing EV demand and supportive government policies. These trends underscore the critical role of BMS in optimizing battery performance, enhancing safety, and facilitating the transition to sustainable energy solutions [6]. The adoption of electrification in mobility and storage systems is widespread globally, with Europe and China serving as major markets [7]. Legislative measures to reduce carbon footprints further bolster the adoption of advanced BMS across various battery technologies, emphasizing their significance in achieving global environmental sustainability goals [8].

The potential market loss due to security vulnerabilities is a major critical issue. BMS, the brain of battery systems, is increasingly connected to the in-vehicular network (IVN), making it one of the prime targets of ethical hackers as well as cybercriminals. Potential consequences include: A compromised BMS could lead to battery failures, thermal runaways, or even fires, posing significant safety concerns. Cyberattacks can manipulate battery data, reducing performance, shorter lifespan, and decreased efficiency. The BMS collects valuable data about vehicle usage, charging patterns, and user behavior. A data breach could compromise sensitive information. Security incidents can damage brand reputation, lead to product recalls, and incur significant financial costs. Increased cybersecurity regulations in the automotive and energy sectors could raise development and compliance costs for BMS manufacturers.

Modern BMS face real cyber threats that extend beyond theoretical risks, affecting vehicle safety, energy efficiency, financial stability, and user privacy. For instance, a cyberattack on the thermal monitoring and management subsystem of a BMS could disrupt temperature regulation, potentially causing overheating. This could lead to catastrophic failure or even an explosion in the worst-case scenario.

As BMS increasingly integrates with electronic and electric mobility systems, its potential to enhance performance and efficiency grows. Cybersecurity plays a pivotal role in developing resilient, intelligent systems. By addressing cybersecurity vulnerabilities, we can transform BMS into secure and reliable cyber-physical systems, thereby improving overall system security and reliability.

This paper emphasizes the need for a robust cybersecurity framework to protect BMS without compromising functionality. By combining deep knowledge of BMS technology with advanced cybersecurity principles, we can develop strategies to mitigate risks and unlock the full potential of BMS. The paper thoroughly examines the cybersecurity challenges facing BMS, particularly in the context of modern energy storage technologies [9].

The rest of the paper is organized as follows: Section II introduces the basics of BMS and the critical role it plays in various applications, such as consumer electronics, electric vehicles, and grid energy storage systems, emphasizing the cybersecurity vulnerabilities that arise from increased complexity and connectivity; Section IV provides an overview of various fault and vulnerabilities of existing BMS; Section III outlines BMS related cybersecurity concerns; whereas, state-of-the-art on cybersecurity measures to secure BMS against cyberattacks is presented in Section V; threat modeling of BMS and proposed framework to manage and mitigate cybersecurity risks throughout the life cycle of automotive systems are presented in VI; and Section VIII discusses emerging trends in BMS technology, such as the application of artificial intelligence (AI) and machine learning (ML), which offer promising solutions for improving real-time monitoring, fault detection, and adaptive security responses.

II. BMS CYBERSECURITY: *BACKGROUND*

BMS has undergone a transformative journey since its inception. Initially, BMS were rudimentary systems primarily focused on preventing overcharging and over-discharging in lead-acid batteries. These early systems were relatively simple, with limited monitoring capabilities. As lithium-ion batteries gained more popularity due to their higher energy density, the complexity of BMS also increased exponentially. The need to balance cell voltages, estimate state-of-charge and state of health, and ensure thermal management became paramount [10]. Contemporary BMS incorporate advanced algorithms, sophisticated sensors, and embedded systems to optimize battery performance, safety, and lifespan. Furthermore, integrating BMS with other vehicle systems, such as powertrain control units and telemetries, has enabled predictive maintenance and remote monitoring.

The growing demands of EVs, renewable energy storage, and portable electronics have driven this evolution. Ever-expanding applications of BMS require intelligent, robust, reliable, and secure BMS solutions to meet the emerging needs of tomorrow. The rapid growth of the electric vehicle industry has been a significant catalyst for BMS [11]. As EVs demand higher energy density, more extended range, and faster charging, BMS has evolved to meet these challenges. Key areas include balancing cell voltages, temperature man-

agement, and estimation, which are crucial for maximizing battery life and performance. BMS is vital in managing charging rates to prevent battery degradation while enabling rapid charging speed. Accurate state-of-charge estimation and range prediction help alleviate user concerns about vehicle range (also known as 'Range Anxiety') and longevity of energy storage systems. BMS enables bidirectional energy flow, allowing EVs and other energy storage systems to supply power to the grid. The intermittent nature of renewable energy sources necessitates efficient energy storage solutions. BMS is essential for managing battery-based energy storage systems and helps regulate power flow between the grid and energy storage systems to maintain grid stability. The BMS can optimize energy storage usage to reduce peak demand charges and efficiently utilize self-generated renewable energy. BMS ensures optimal battery performance and longevity in stationary applications.

Looking ahead, future advancements in BMS technology hold promise for further enhancing battery performance and system efficiency [12]. Advanced cell monitoring technologies will enable BMS to conduct detailed diagnostics and anomaly detection [13]. This is expected to facilitate the early identification and mitigation of potential issues before they escalate into more significant problems. Additionally, enhanced integration with vehicle systems [14], such as chargers and thermal management systems, will optimize charging strategies and overall system performance, contributing to greater energy efficiency and prolonged battery life [15]. One of the most significant advancements in this field is the development of wireless BMS. This technology eliminates the need for physical wiring between the battery and the management system, reducing complexity and improving reliability. However, this wireless connectivity also opens new avenues for potential security threats. The BMS interacts with vehicle control systems, powertrain controllers, and telematics control units (TCU) to manage energy flow within the vehicle systems, but the interconnectivity also introduces significant cybersecurity risks. As BMS communicates with other vehicle subsystems via CAN Bus, Ethernet, or wireless protocols, a compromised BMS can serve as a gateway for cyberattacks, enabling hackers to manipulate SOC or SOH data, leading to battery degradation, overheating, or even thermal runaway. The wBMS further increases vulnerabilities, as attackers can remotely inject malware, disrupt V2G functions, or execute DoS attacks, potentially causing system failures. Additionally, unauthorized access to BMS data may expose sensitive user information, charging habits, and vehicle diagnostics, posing serious privacy risks.

A. KEY MODULES OF A BMS

An overview of critical modules/subsystems/units of a BMS is provided in the following:

Cell Balancing Unit (CBU) [16]:
- It ensures uniform charging and discharging of all battery cells.
- It prevents overcharging or deep discharge of individual cells using passive balancing (energy dissipation as heat) and active balancing (energy transfer between cells).

State of Charge (SOC) Estimation Unit [17]:
- It accurately determines the remaining battery capacity and range estimation.
- It utilizes various algorithms and sensors (current, voltage, temperature) to calculate SOC.

State of Health (SOH) Monitoring Unit [18], [19]:
- It assesses the overall battery condition and degradation and predicts battery life.
- It enables proactive maintenance planning and battery replacement strategies.

Thermal Management Unit [20]:
- It aims to regulate battery temperature within optimal operating range to prevent overheating, which can lead to capacity loss, safety risks, and reduced battery life.
- It employs cooling systems (liquid or air) to dissipate heat and lower cell temperature.

Overcharge and Over-discharge Protection Unit:
- It aims to prevent battery damage from excessive charging or discharging.
- It implements safety measures to protect the battery and vehicle.

Cell Voltage Monitoring Unit [21]:
- It continuously tracks individual cell voltages.
- It detects imbalances and initiates cell balancing.
- It prevents cell damage and improves battery life.

Current Monitoring Unit [22]:
- It measures battery charging and discharging currents.
- It protects against excessive currents that can cause overheating and safety hazards.

Communication Unit:
- It exchanges data with other vehicle systems (e.g., powertrain control unit, infotainment system).
- It enables remote monitoring and diagnostics.
- It facilitates integration with charging infrastructure.

B. KEY FUNCTIONALITIES OF BMS IN RENEWABLE ENERGY STORAGE SYSTEMS

- Energy Optimization: BMS enhances energy efficiency by monitoring battery health and optimizing charging/discharging cycles to align with supply and demand fluctuations.
- Grid Stabilization: By regulating battery charging and discharging, BMS contributes to grid stability by balancing power supply and demand, especially for intermittent renewable energy sources.
- Peak Shaving: BMS helps reduce electricity costs by discharging stored energy during peak demand periods, lowering the grid's overall load.
- Safety: BMS prioritizes safety by incorporating features that prevent battery failures, such as overcharging, over-discharging, and overheating protection.

C. KEY ROLES OF CYBERSECURITY THREATS TO BMS

- Data Exposure: Sensitive information about battery systems can be stolen, misused, or sold.

- System Interference: Hackers can manipulate BMS functions to compromise vehicle performance or safety.
- Service Disruption: Attacks can render BMS inoperable, causing system failures and inconveniences.
- Supply Chain Risks: Malicious components in the supply chain can create vulnerabilities in BMS.

III. CYBERSECURITY CONCERNS

With the BMS becoming more interconnected and remotely accessible, cybersecurity professionals have started developing countermeasures to safeguard it against cyberattacks. Cybersecurity of BMS become a key requirement for system design engineers and cybersecurity professionals [23]. Bad actors can take advantage of known vulnerabilities in the BMS to disrupt the operation of the battery, which could also lead to substantial financial losses for the stakeholders. Unauthorized access or tampering with BMS and its subsystems can have dire consequences. In a security breach incident, the repair costs of a compromised BMS can be in the tens of millions of dollars. This includes the cost of identifying the breach, rectifying the damage, and implementing measures to prevent future attacks. Therefore, investing in robust security measures for BMS is necessary and financially prudent. To mitigate these risks effectively, best practices must be followed during the product design, development, and testing. These include regularly updating software, implementing robust authentication protocols, network segmentation, monitoring system logs, and encrypting data transmission. Another crucial aspect to consider is the security measures the BMS provider implements. They must have robust security protocols to protect against potential cyber threats.

The functionalities of modern BMS extend far beyond the basic protective functions. For instance, it actively manages battery temperature to prevent overheating, which can significantly degrade battery health and lifespan. BMS also controls the Depth of Discharge (DOD) to minimize cell degradation over time [24]. A deeper DOD allows more energy to be extracted from the battery, causing cells to undergo additional stress. By regulating DOD, BMS helps balance maximizing usable battery capacity and prolonging battery life.

Recent innovations in BMS technology include the adoption of wireless architectures. These architectures enhance communication reliability within complex battery systems, improving data accuracy and resilience. Wireless BMS (wBMS) solutions also offer additional benefits, such as simplifying installation by reducing wiring complexity and enabling more flexible battery pack designs, which are critical for evolving applications in electric mobility and stationary energy storage systems. The future holds even more promise with the integration of cloud connectivity. This is expected to revolutionize BMS capabilities by enabling real-time remote monitoring, predictive maintenance, and data-driven optimization strategies. Cloud connectivity facilitates continuous improvement in battery management strategies based on real-world usage data, enhancing reliability and operational efficiency over time. Standardization efforts across manufacturers is expected to streamline BMS development further, promote interoperability, and accelerate innovation, fostering broader market adoption and integration across diverse applications [1].

The advances in BMS technology have also introduced new challenges. For instance, modern BMS are susceptible to various faults and vulnerabilities that can significantly impact EV performance and passenger safety [25]. These faults and vulnerabilities include:

- **cell imbalance** refers to when some cells in a battery pack degrade faster than others, leading to uneven utilization and premature aging of the entire pack.
- **Thermal runaway** is another issue where battery overheating can trigger a dangerous chain reaction, causing the battery to generate more heat as its temperature rises [26]. BMS is crucial in preventing thermal runaway through temperature monitoring and regulation.
- **Voltage inconsistencies** refer to variations in the voltage levels of individual cells within a given battery pack. Other factors, such as manufacturing differences, aging, temperature differences, and varying states of charge (SoC) among the cells, can also cause voltage inconsistencies. These inconsistencies can lead to imbalances that can affect the overall performance, lifespan, and safety of the energy storage system.
- **communication errors** refer to disruptions in wired or wireless communication between various components of the BMS or between the BMS and other systems. These errors can significantly impact the performance, safety, and reliability of the energy storage system. Hardware faults, software bugs, interference, or improper configurations are the main factors behind communication errors.

These inconsistencies degrade the overall performance of BMS [27], and addressing them requires advanced diagnostic capabilities and robust fault-tolerant designs to ensure reliable and resilient BMS in diverse and demanding operational environments. While BMS offers substantial advantages in energy efficiency, performance optimization, and enhanced safety, their vulnerability to faults, cyberattacks, and operational risks presents considerable concerns. Malicious attacks targeting BMS control systems or compromising data integrity could disrupt operations or compromise vehicle and user safety. Moreover, operational faults or failures in BMS can lead to significant economic losses, downtime, and even safety hazards. This underscores the critical need for stringent cybersecurity measures and fault-tolerant designs [28].

BMS represents a cornerstone of modern energy storage solutions. Its vital role in ensuring efficient, safe, and long-lasting battery operation spans various applications. As the technology continues to evolve, addressing challenges like faults, vulnerabilities, and cybersecurity threats will be crucial to unlocking the full potential of BMS in shaping

a sustainable energy future. The following section will delve deeper into the Faults and Vulnerabilities Associated with BMS, exploring the specific technical issues and potential consequences. The cybersecurity threats to BMS can be broadly categorized into three main categories: (i) communication-based, physical-based, and software & data-based attacks. Table 1 categorizes cybersecurity threats to modern BMS, their description, and their impact on BMS.

IV. BMS FAULT AND VULNERABILITY ANALYSIS

Despite their critical role, BMS is vulnerable to various faults and vulnerabilities that can significantly impact its performance, reliability, and safety. These issues can broadly be categorized into hardware and software faults, each posing distinct challenges.

A. HARDWARE AND SOFTWARE FAULTS

Hardware faults within BMS include sensor failures [29], power supply irregularities [30], and wiring defects. Sensor malfunctions, such as inaccuracies in temperature or voltage readings, can lead to incorrect battery management decisions, potentially compromising overall system safety. Power supply fluctuations or failures may disrupt BMS operation, while wiring issues can result in short circuits or intermittent connectivity, undermining system reliability and performance.

On the software side, BMS are vulnerable to faults stemming from bugs in firmware or algorithmic errors [31]. These faults can appear as inaccuracies in state estimations, communication failures [32] between BMS components, or vulnerabilities exploited by malicious software [33]. Addressing software faults requires thorough testing, regular updates, and adherence to secure coding practices to reduce risks and ensure robust BMS performance under various operational conditions.

Shown in Figure 2 is a detailed block diagram outlining various categories of faults that may affect a BMS. These faults are broadly categorized into three main categories:

- Malfunction Faults
- Hardware Faults, and
- Application Faults

Shown in Figure 1 is the illustration of BMS failure mode analysis and their cascading impact. It categorizes failure modes into various faults, including sensor faults, balancing circuit defects, overcharging/undercharging, unprotected hardware, thermal management failures, firmware faults, and communication errors. These failures affect critical components such as temperature/voltage/current sensors, cell balancing and pack monitoring units, control boards, interface circuits, and communication ports. The faults propagate to subsystems, including SOC/SOH estimation modules, charge controllers, thermal management, cybersecurity, and communication regulation. Ultimately, these failures lead to severe system-level impacts, including incorrect battery state reporting, cell voltage imbalance, thermal stress, misleading fault detection, data loss, and even system hijacking. The visualization highlights the interconnected nature of failures within BMS, emphasizing the need for robust fault detection and mitigation strategies.

Malfunction faults include issues stemming either through the user interface or physically. These include under-discharging [34], cell imbalance, communication errors, overcharging, and over-temperature conditions.

Hardware faults primarily stem from manufacturing defects occurring before installation or after a certain period of operation. Examples include damaged printed circuit boards (PCBs), wiring disconnections, sensor faults, and defective switches.

Application faults are bugs within the BMS system or firmware that result during system updates or installations. These faults include software/firmware issues, unprotected hardware components, onboard interface irregularities, data storage miscommunications, network errors, and calibration issues.

B. VULNERABILITIES

Current challenges in BMS predominantly stem from the emergence of dynamic faults and vulnerabilities that cybercriminals can exploit. Bad actors can exploit these vulnerabilities in BMS software or communication protocols to manipulate system functions, alter sensor data, and/or compromise data integrity [9]. The complexity and rapid evolution of attack surfaces pose significant challenges to conventional fault detection and mitigation strategies. Consequently, adaptive cybersecurity measures, including real-time threat intelligence and continuous monitoring, are essential to safeguard BMS operations against malicious interventions [35].

Future advancements in BMS technology and battery systems will expand existing attack surfaces of BMS. As BMS become more interconnected and integrate advanced technologies such as AI and ML [36], they may face novel risks such as AI model biases, data poisoning attacks, or sophisticated cyber attacks targeting AI-driven decision-making processes. Proactive research into adversarial AI/ML models, secure integration frameworks, and standardized protocols for secure data exchange within BMS will be crucial to mitigating these emerging risks effectively. Understanding the distinction between static and dynamic faults is pivotal for assessing the impact of cyberattacks on BMS. Typically predictable and attributable to hardware or software defects, conventional fault detection methods can often mitigate **static faults**. In contrast,**dynamic faults** arise from external interference, such as unauthorized access or malware infiltration, presenting unpredictable and evolving threats to BMS integrity and operational safety. Effective mitigation strategies necessitate adaptive cybersecurity frameworks, rapid incident response capabilities, and ongoing research into advanced anomaly detection techniques to address the evolving landscape of cyber threats targeting BMS [37].

TABLE 1. Categorization of Cybersecurity threats in BMS.

Category	Threat Type	Description	Impact on BMS
Communication Attacks	Denial-of-Service (DoS)	Flooding CAN Bus or IVN with excessive messages	Disrupts safe charging/discharging cycles
	Sniffer Attacks	Eavesdropping on BMS communication to intercept sensitive data	Data leakage, exposure of battery parameters
	Man-in-the-Middle (MITM)	Intercepting and modifying messages between BMS and vehicle units	False data injection, incorrect battery state reports
	Jamming Attacks	Wireless interference affecting wBMS communication	Data loss, incorrect charging/discharging decisions
Physical Attacks	Hardware Tampering	Unauthorized modifications to BMS hardware	Malfunctions, data theft, system hijacking
	Electromagnetic Interference (EMI) Fault Injection	Using EMI to disrupt BMS circuits	Sensor malfunctions, false fault triggers
	IC Counterfeiting & Tampering	Insertion of fake or modified ICs into BMS	Reduced reliability, hidden malware risks
	Temperature Sensor Manipulation	Altering sensor readings to trigger false alarms	Overcharging, overheating risks
Software & Data Attacks	Malware Injection	Injecting malicious software via firmware updates or physical access	Unauthorized access, system control manipulation
	Ransomware Attacks	Encrypting critical BMS data to demand ransom	System lockout, disrupted battery management
	Trojan Horse	Disguising malware as legitimate software updates	Data theft, silent BMS manipulation
	Modeling Attacks	Exploiting BMS algorithms for inaccurate battery parameter estimation	False SOC/SOH readings, performance degradation
	Timestamp Manipulation	Altering event timestamps in BMS logs	Misleading fault logs, incorrect charging cycles

Addressing faults and vulnerabilities in BMS is essential to ensure reliability, safety, and performance of battery-powered applications. A multidisciplinary approach integrating advanced fault diagnosis techniques, robust cybersecurity measures, and continuous innovation in BMS technology will be critical in mitigating risks and enhancing the resilience of BMS against evolving threats. By advancing our understanding of BMS attack surfaces and vulnerabilities and designing, developing, and implementing proactive mitigation strategies, we can foster the sustainable advancement and secure deployment of battery-powered systems across various applications. In cybersecurity terminology, an **attack vector** represents a specific method or pathway through which an adversary gains unauthorized access to a system or network. These vectors exploit vulnerabilities inherent in software, hardware, or human factors to achieve malicious objectives, such as data theft, system disruption, or manipulation of [38] and [39]. BMS, which play a critical role in monitoring and managing the performance and safety of battery packs in electric vehicles and other applications, are particularly susceptible to such threats. Common attack vectors targeting BMS include malware injection, where malicious software is introduced to compromise system integrity; **electromagnetic interference** (EMI) fault injection, which employs electromagnetic fields to induce operational faults; **temperature sensing manipulation**, where false temperature data is injected to cause malfunction or damage; and **jamming**, which disrupt the communication signals within the BMS [40], [41]. These attack surfaces can result in severe consequences, such as battery overheating, fire hazards, or total system failure. This paper examines using EMI fault injection as a critical

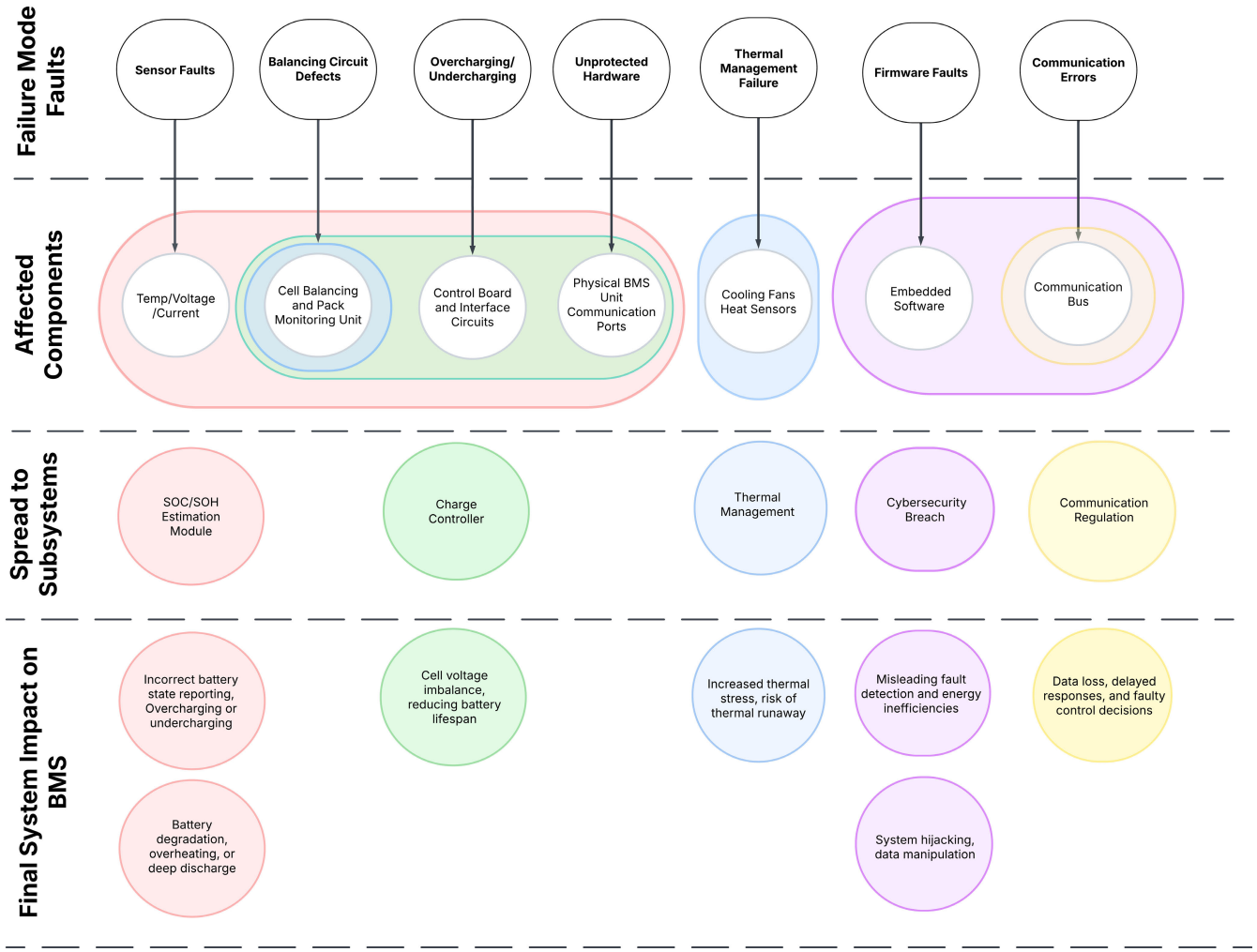


FIGURE 1. Illustration of failure mode analysis of BMS sensors and their cascading impacts.

attack vector, demonstrating how attackers can induce faults in the BMS to provoke erroneous behavior or disrupt normal operations. This analysis underscores the imperative for robust cybersecurity measures to protect BMS from sophisticated attacks and ensure battery-powered systems' safe and reliable operation.

Shown in Figure 3 is an illustration of a comprehensive exploration of potential security vulnerabilities in BMS, such as Denial-of-Service, Sniffer, Trojan, Modeling, Ransomware, and Sensor Data Tampering attacks

- **Denial-of-Service (DoS) attacks** disrupt BMS operations by flooding the Controller Area Network (CAN) with excessive messages [38], overwhelming the system and disrupting critical functions such as safe charging/discharging cycles, temperature monitoring, and accurate SoC estimations. These attacks can also interfere with communication between the BMS and other vehicle systems, potentially causing malfunctions or data loss.
- **Sniffer attacks** involve passive eavesdropping on BMS communication to intercept sensitive data like battery health metrics, SoC, and unique identifiers [9], [42], exposing critical information to unauthorized parties and facilitating potential data exploitation and targeted attacks.
- **Trojan attacks** infiltrate BMS systems disguised as legitimate software [35], [43], enabling attackers to steal confidential data or manipulate system operations, compromising battery performance, introducing unsafe charging practices, and destabilizing system reliability. Detecting malware is challenging due to its deceptive nature, necessitating robust security measures and regular software updates.
- **Modeling attacks** exploit vulnerabilities in the internal models of BMS for estimating battery parameters, injecting false data, or manipulating algorithms to mislead the BMS into unsafe conditions, such as incorrect SoC readings or compromised thermal management.

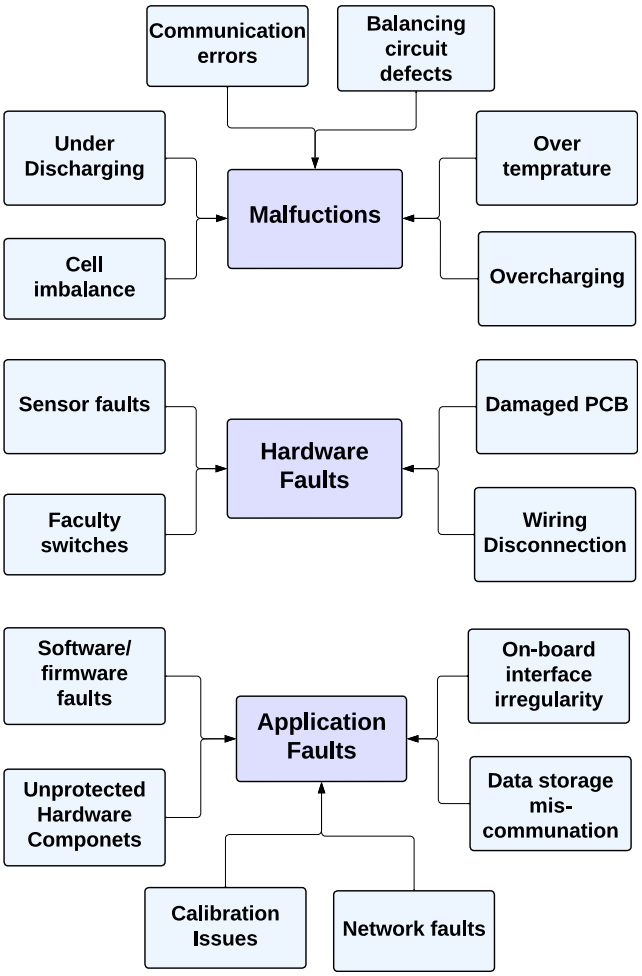


FIGURE 2. Comprehensive block diagram of battery management system faults.

Effective noise mitigation involves implementing shielding, proper grounding practices, and filtering techniques within the BMS design.

- **Ransomware attacks** a type of malware attack encrypts critical BMS files, rendering the system inaccessible and disrupting functions such as battery monitoring [44], safety protocols, and data management, posing risks like overheating or battery failure. Mitigating ransomware threats requires proactive measures such as regular backups, robust cybersecurity protocols, and rapid incident response strategies.
- **Sensor data tampering attacks** exploit vulnerabilities in BMS communication protocols or physically tamper with temperature sensors to manipulate readings [38], [45], misleading the BMS into incorrect thermal management decisions, and endangering battery safety and performance.

Each type of attack presents unique challenges and risks to BMS security, underscoring the critical need for comprehensive cybersecurity strategies and ongoing vigilance to safeguard vital battery systems across diverse industries.

V. BMS SAFETY: *RELATED WORK*

Various researchers have been investigating BMS safety and security issues [43], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [45], [59], [44], [58], [60], [61], [62]. A brief overview of state-of-the-art BMS safety and security is provided in the following subsectionV-A.

A. BMS SAFETY AND SECURITY: STATE-OF-THE-ART

BMS is crucial for second-generation HEVs, EVs, and renewable energy storage systems. They perform various tasks, such as monitoring voltage and current, estimating charge and discharge, equalizing the voltage in the cells, protecting the battery, and managing temperature conditions and battery data. Various battery models, including electric, thermal, and electro-thermal models, have been comprehensively analyzed in [46]. Kumar et al. in [46] presented the state estimations of battery charge and health and discussed different battery charging approaches and optimization methods. In addition, Kumar et al. in [46] also examined various cell balancing circuit types, their advantages and disadvantages, and identified research gaps in BMS safety and security.

In high-power applications such as EVs and HEVs, the BMS ensures battery safety and power [47]. Manas et al., [47] propose an architecture that includes a hardware demonstration and a simulation of the continuous on-time control approach for systematically measuring voltage, current, and temperature in EVs. A single-ended primary-inductance converter (SEPIC) DC-DC converter, Analogue Front End (AFE), and balancing circuits supply the proposed congregated BMS process optimally. The effectiveness of the proposed congregated design performance is validated through meter and sensor measurements for voltage, current, and temperature. The need for accurate prediction of the battery's SOH and timely detection of anomalies for effective battery management is addressed in [48].

Lee et al. in [48] proposed an approach for online real-time SOH prediction and anomaly detection for rechargeable batteries throughout their life cycles. The Presentation includes [48] a model-based prediction of battery states under normal aging, a reference for anomaly detection. The model parameters and uncertainties are updated cyclically and temporally based on the predicted SOH. The authors also proposed a method for SOH prediction under realistic conditions such as inter- and intra-cycle variations in load current and nonstandard charging and discharging practices.

A comprehensive analysis of BMS components and their intended functionalities is presented in [49]. A BMS acts as the central nervous system for a battery pack to continuously monitor critical aspects like temperature, voltage, and current [49]. It also facilitates communication between the battery and other components within the system.

Lelie et al. in [49] presented an overview of the essential building blocks of a BMS, including sensors, the analog front end, and the BMS master module. Notably, the choice

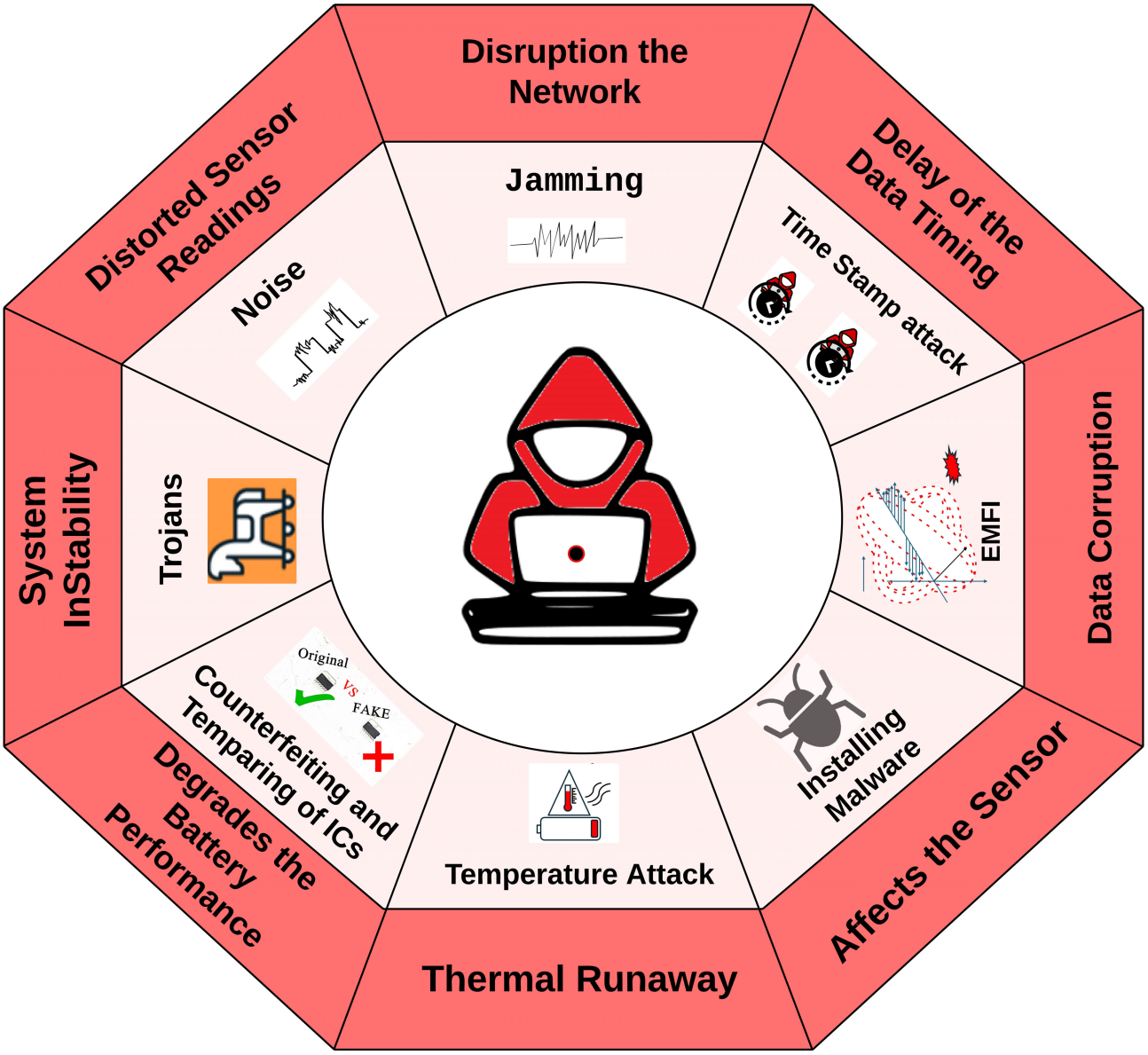


FIGURE 3. Potential security weaknesses (indicated in light red) and dangers in BMS, emphasizing the risks associated with various forms of attacks (denoted in dark red).

of BMS integrated circuits (ICs) depends on the specific application. Some ICs cater to compact, single-cell devices, while others are designed to handle larger battery packs comprised of multiple cells.

1) BMS FAULT ANALYSIS

Several studies on BMS fault analysis [50], [51], [52], [53] have been focused on diagnosing and analyzing overcharge and over-discharge faults in LIBs, mainly for automotive applications. For instance, Zheng et al. in [50] used a dynamic simulation model to investigate these faults, concluding that fault diagnosis analysis of LIBs can yield effective results and is valuable for diagnosing LIBs with varying parameters. This study [50] emphasized that overcharge and over-discharge faults in automotive LIBs can negatively impact the battery's performance, suggesting that automobile manufacturers should pay more attention to these issues.

Xie et al. [51] investigated BMS faults and their impact in the context of vehicle safety and reliability of EVs. Specifically, this study focused on testing the accuracy, timeliness, and reliability of BMS fault responses using a HIL simulation environment and an actual test environment. The study examined different BMS responses under battery system fault conditions such as over-charge, over-discharge, over-temperature, and over-current.

Schmid et al. in [52] proposed a novel data-driven approach to fault diagnosis in the BMS of EV batteries. This study presented a method for detecting and localizing

faults based on a statistical evaluation of single-cell voltages using Principal Component Analysis (PCA). The research highlights the capability of their method to learn and generalize, as demonstrated by an artificial parameter change and cross-validation. Likewise, Zhen et al. in [53] presented a unique approach to sensor fault diagnosis in Li-ion battery systems was presented. This work utilized hybrid system modeling to tackle the challenge of diagnosing sensor faults in BMS and modeled the battery system as a hybrid system using stochastic automata, defining various discrete states to represent the normal and faulty states of the system, by employing an unscented particle filter algorithm, along with prior discrete state transitions, to estimate the most probable discrete states of the system, thereby providing diagnostic outcomes. The innovative method in [53] offers a promising solution for sensor fault diagnosis in complex Li-ion battery systems.

Cheng et al. [54] proposed a framework to utilize 50 current-voltage samples during the startup phase of a LIB system to detect two common types of sensor faults. The effectiveness of this method in diagnosing current sensor faults was experimentally validated, achieving a low miss alarm rate (MAR) and false alarm rate (FAR). A diagnostic scheme for LIB systems used in hybrid electric aircraft was introduced, employing a systematic structural analysis methodology to design the fault diagnosis algorithm. The proposed diagnostic scheme was validated using a SIL approach, demonstrating its ability to successfully detect and isolate individual cell faults (internal short circuit), connection faults (external short circuit), and sensor faults within the LIB system.

Fedorova et al. in [55] provided a comprehensive review of fault diagnosis technologies was provided for LIBS. Authors in [55] discussed the mechanisms, features, and diagnosis procedures of various faults in LIBS, including internal battery faults, sensor faults, and actuator faults. This paper also discussed future trends in developing fault diagnosis technologies for safer battery systems. Similarly, modern cyber-physical battery systems (CPBS) have evolved due to the data exchange facilitated by the IoT in [56], leading to potential vulnerabilities. A security analysis of battery systems used in various IoT applications is presented in [38]. The authors argued that it is crucial to ensure the correct functioning of batteries and prevent security threats targeting the battery systems.

The transition from conventional BMS safety and security mechanisms to modern AI-driven and cloud-based approaches marks a significant evolution in battery management technology. Traditional fault detection relied heavily on static threshold-based models, often leading to delayed or lower fault identification rates. In contrast, AI-based predictive analytics have enabled real-time diagnostics, reducing failure rates and enhancing battery lifespan. Similarly, blockchain-based security, intrusion detection systems, and adaptive AI models have supplemented conventional cybersecurity measures, such as crypto-based authentication methods, which provide more robust protection against cyber threats. Furthermore, localized BMS designs have been outpaced by cloud-based architectures, improving scalability and enabling remote monitoring capabilities. These advancements underscore the growing need for integrating AI-driven approaches into BMS to ensure higher efficiency, reliability, and security in modern battery-powered systems.

B. SECURING THE BMS

The safety and efficiency of BMS in LIBs have been the focus in [57], [58], [59]. A comprehensive BMS including modern parameters like fast charger, battery aging diagnosis, charge estimation, SOC balancing, and predicting SOH of the cells are discussed in [57]. An in-house trained ANN model for charger utilization is proposed to use a single-inductor and single-input-dual-output architecture to achieve charge balancing among battery cells. This method aims to reduce the charging time, slow the battery aging process, and significantly suppress the temperature variations of battery cells, which is beneficial for charge balancing. The critical role of BMS in ensuring the safety and efficiency of batteries was emphasized in [58]. With the increasing complexity of BMS, expanding interconnections between batteries and their applications, and the emergence of cloud-based energy storage systems, there are growing concerns about battery cybersecurity. The authors in [58] proposed a novel and robust security approach to design a BMS to prevent misuse and undesired manipulation of battery equipment and data. A model-based diagnostic scheme for real-time detection, isolation, and estimation of sensor faults in the BMS has been discussed in [59]. The authors highlighted the importance of accurate sensor readings for the safety and reliability of the battery. The proposed diagnostic scheme uses sliding mode observers designed based on the electrical and thermal dynamics of the battery.

Kim et al. in [43] proposed a blockchain technology-based method to protect BMS from malicious cyber-physical attacks and ensure the secure utilization of battery systems for numerous applications in cyber-physical environments. The potential of the IoT and cloud computing technologies in advancing BMS has been presented in [9]. The authors provided an overview of potential cyber-attack schemes and proposed defense strategies to protect IoT-enabled BMS systems from these malicious attacks. Sripad et al. in [45] highlighted vulnerabilities of EV battery packs to cyberattacks on auxiliary components, emphasizing that EV batteries' unique and critical nature amplifies the risk of cyber threats. The authors developed a systematic framework to model these cyberattacks and analyze their impact on EV batteries, finding that these attacks could deplete a battery pack by up to 20 percent per hour in the short term. The increasing use of BMS in energy storage systems is addressed in [44] due to the rise of renewable energy and EVs and the corresponding increase in cybersecurity threats. The study also mentions solutions like encryption, access controls, and

security protocols and emphasizes best practices such as regular software and firmware updates.

EMI susceptibility of BMS used in Li-ion and lithium-polymer (LiPo) battery packs in EVs and HEVs has been investigated in [60]. This study provides insights into the electromagnetic vulnerabilities of BMS in the context of EVs. Crocetti et al. in [58] discussed the critical role of BMS in ensuring the safety and efficiency of batteries. This paper emphasized the need to secure BMS against cyber threats. It proposed a novel security approach to design and develop robust BMSs against misuse and undesired manipulation of battery equipment and sensor data. In addition, recent studies [58], [60] have investigated foundational principles for cybersecurity for EVs.

The concept of a fault template attack based on fault probability, a powerful side-channel attack method utilizing leaked information from various side channels, was also discussed in [63]. Efficient and effective fault diagnosis methods for battery systems were presented in [61]. A detailed study of communication protocol between BMS and energy storage cells during the charging phase was also presented in [61]. A comprehensive solution for fault detection and real-time monitoring of charging piles based on embedded devices was presented in [61]. Novel architectures, advancements in cloud computing, and the application of AI are shaping the future trends in BMS, were proposed in [62]. The proposed architecture proposed in [62] relies on the power/data time division multiplexing transmission technique, simplifying wiring using a common bus to transfer power and data simultaneously. This system, composed of a pack management unit and several cell management units (CMUs), can be integrated with a battery cell to create an intelligent cell. Cloud-based BMS (CBMS) and cyber-physical systems are linked to offer significantly higher computational resources, leading to improved performance and safety of Battery Energy Storage Systems (BESS). The paper [50] highlights the cybersecurity vulnerabilities of CBMS and discusses potential countermeasures to protect CBMS against cyberattacks.

VI. THREAT MODELING: COMMON ATTACK VECTORS FOR MODERN BMS

As BMS technology integrates with the ever-expanding digital landscape, it becomes increasingly vulnerable to cyberattacks. This section discusses attack surfaces for BMS and its subsystems. Exposing potential vulnerabilities is expected to highlight the importance of developing countermeasures to protect BMS against potential exploits. Understanding the evolving cyber threat landscape is paramount for manufacturers, developers, and users of BMS technology. This section aims to highlight the need to develop robust countermeasures and implementation best practices by identifying the malicious tactics employed by attackers. This proactive approach is essential to safeguard the integrity and functionality of BMS, ultimately ensuring the safety and reliability of the devices they manage.

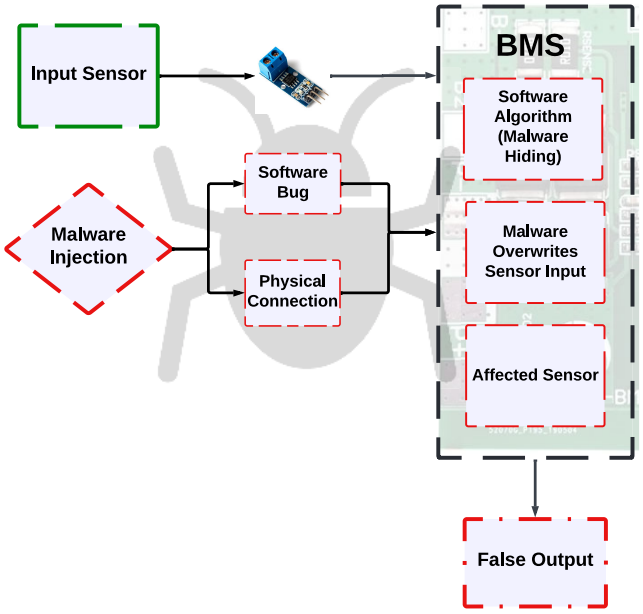


FIGURE 4. Malware Injection and Sensor Manipulation in BMS: Illustration attack vectors for BMS, including introducing malicious software and altering sensor data. These cyberattacks can compromise battery health, performance, and safety and expose sensitive vehicle information.

A. MALWARE ATTACKS

Malware injection poses a significant risk to the integrity and functionality of BMS. Attack vectors include physical access, where attackers can directly upload malware if physical security measures are breached. This can occur in publicly accessible areas or vulnerable vehicle environments. Another method involves exploiting software update processes; malware can be embedded within seemingly legitimate updates, leveraging user trust to infiltrate the system. Verifying updates using digital signatures is essential to prevent tampering and ensure updates originate from trusted sources [38]. Wireless connectivity in BMS, common in EVs for remote monitoring and updates, also introduces vulnerabilities. Attackers can exploit weaknesses in communication protocols or conduct man-in-the-middle attacks [9], [42] to intercept and manipulate data transmitted between the BMS and the network. These exploits highlight the need for robust security measures in wireless communication protocols and networks to prevent unauthorized access and data integrity verification.

The impact of malware on BMS sensors is profound and varied, potentially compromising critical operations. Malware can manipulate sensor data, misleading the BMS into making unsafe decisions, such as overcharging batteries based on falsified voltage readings. This manipulation can lead to overheating, damaging both the battery and the sensors. Additionally, malware can also disrupt the operations of thermal management systems and impair the ability of BMS to regulate temperature, risking further sensor damage and compromising overall system reliability.

Understanding the specific impacts of malware on BMS sensors depends on the attack type and the design of the BMS itself. Malware targeting communication protocols may distort sensor readings, leading to erroneous control actions. Conversely, attacks on BMS firmware could alter control algorithms, causing the system to respond inappropriately to valid sensor data. Given these risks, developing and implementing robust cybersecurity measures is paramount. This includes securing communication protocols, fortifying update processes, and enhancing physical security measures to mitigate the potential impacts of malware on BMS sensors, ensuring these critical systems' continued safety and reliability. In conclusion, the threat of malware injection in BMS presents significant challenges that require ongoing research and vigilance. By addressing vulnerabilities through comprehensive cybersecurity strategies, we can enhance the resilience of BMS against evolving cyber threats, safeguarding their essential role in modern energy systems and transportation.

Shown in Figure 4 is an illustration of malware-related vulnerabilities of BMS targeting BMS sensing layer functionalities. Malware injection can occur through various means, including software or firmware updates and unprotected physical connections during maintenance. Once injected, the malware explicitly targets the sensors within the BMS. For instance, a current sensor could be manipulated to produce altered or false data readings, disrupting the accuracy and timing of its measurements. Subsequently, the compromised sensor data is transmitted to the BMS, which is processed as valid information. Unaware of the manipulation, the BMS incorporates this data into its calculations, potentially leading to inaccurate outputs. These false outputs can result in incorrect decisions regarding battery management tasks such as charging or discharging rates. Such inaccuracies pose a risk to the efficiency of the battery system and safety risks to the overall operation. This depiction underscores the critical importance of robust and secure BMS. Safeguarding against malware attacks requires secure software and firmware update processes, ensuring updates are obtained from verified sources and are free from tampering. Similarly, protecting physical connections during maintenance procedures is essential to prevent unauthorized access and malware injection. Implementing stringent measures for detecting and mitigating data manipulation within the BMS is vital to maintaining system integrity and reliability. Figure3. emphasizes the vulnerabilities of BMS sensors to malware-induced manipulation and highlights the necessity for proactive cybersecurity strategies.

By fortifying defenses against malware attacks through secure update protocols and vigilant maintenance practices, industries can mitigate cyber threats and ensure the performance and safety of battery-powered systems. Secure software and firmware updates should be enforced in BMS using digital signatures, secure boot mechanisms, and encrypted communication channels to prevent unauthorized modifications. Access control measures, such as multi-factor authentication (MFA), role-based access control (RBAC), and IDS, can restrict unauthorized access and detect anomalies in real-time. Hardware security should also be reinforced with tamper-proof components, secure debugging interfaces, and encrypted storage to prevent direct hardware-based malware attacks. Additionally, AI-driven anomaly detection approaches and periodic penetration testing can proactively identify and mitigate vulnerabilities. Integrating secure firmware updates, strong authentication, encrypted communications, and AI-driven BMS monitoring systems have the potential to safeguard BMS against malware threats and ensure its safe and reliable operation.

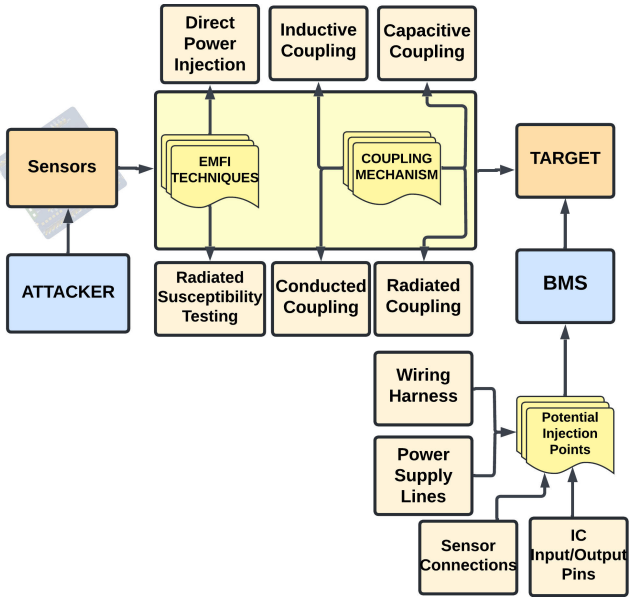


FIGURE 5. Depiction of EMI Fault Injection Attack: This Figure illustrates how to compromise a system by introducing electromagnetic interference. EMI can manipulate the behavior of electronic components, potentially leading to incorrect data processing, system malfunctions, or security breaches.

B. ELECTROMAGNETIC INTERFERENCE(EMI) FAULT INJECTION ATTACK

Electromagnetic Fault Injection (EMI-FI) is a technique used to evaluate the vulnerability of electronic systems, such as BMS, to EMI. It involves deliberately introducing controlled electromagnetic energy into the BMS to observe its response. This can expose weaknesses in the system that could be exploited by an external electromagnetic field [64]. EMI-FI works by disrupting the normal flow of electricity within the BMS circuits. The injected EMI can induce unwanted voltages or currents in sensitive components, including sensors and actuators, potentially causing them to malfunction [65]. This can lead to various consequences, depending on the severity and location of the interference. For example, EMI-FI might cause the BMS to misinterpret sensor readings, leading to inaccurate data about battery health or state of charge. In a worst-case scenario, it could trigger safety

shutdowns or even cause permanent damage to the BMS or connected battery.

Two primary EMI-FI testing techniques exist: (i) direct power injection and (ii) radiated susceptibility testing, as shown in Figure 5. Direct power injection involves applying a controlled electrical surge directly onto specific BMS circuitry points, often targeting the front-end Integrated Circuits (ICs) [66]. This approach, while capable of simulating certain fault scenarios, is risky due to the delicate nature of electronic components. Tools like chip shouters can be used for this method, but their application can cause permanent damage and are generally not recommended for practical EMI-FI testing on BMS. A safer alternative is radiated susceptibility testing, which exposes the entire BMS to a controlled electromagnetic field generated by an antenna or chamber. This method simulates real-world conditions where the BMS might encounter EMI from external sources such as radio transmitters, high-power electrical lines, or even intentional jamming attempts. By carefully controlling the radiated EMI's intensity, frequency, and duration, researchers can evaluate the robustness of BMS and identify potential weaknesses in its shielding or design that could be exploited in real-world scenarios. This approach offers a more comprehensive assessment of the susceptibility of BMS to EMI without the risk of permanent damage associated with direct power injection [67].

EMI can infiltrate a BMS through various coupling mechanisms, each presenting potential injection points for attackers [68]. Conducted coupling utilizes the conductive pathways of BMS, such as wires or circuit board traces, to transmit EMI. While targeted injection at these points offers precision, it necessitates a deep understanding of the specific BMS design. In contrast, radiated coupling exposes the entire BMS to electromagnetic waves, mimicking real-world scenarios like radio transmitters or intentional jamming attempts. Inductive coupling arises when a nearby conductor's changing magnetic field induces unwanted currents in BMS components. This can occur if the BMS is positioned close to a strong source of electromagnetic radiation—finally, capacitive coupling results from the electric field between adjacent conductors within the BMS. Rapid voltage changes on one conductor can induce unintended currents in the other, potentially disrupting operation. Considering these diverse coupling mechanisms, potential injection points for EMFI attacks include wiring harness (conducted coupling), sensor connections (disrupting readings), Integrated Circuit (IC) input/output pins (directly affecting IC operation), and power supply lines (disrupting power flow and potentially damaging components). By understanding these coupling paths and injection points, researchers can design more robust BMS with improved shielding and immunity to EMI-based attacks.

A structured defense approach is essential to enhance BMS resilience against EMI attacks. Implementing electromagnetic shielding using conductive enclosures and ensuring proper grounding techniques can significantly reduce EMI susceptibility. Additionally, low-pass filters, ferrite beads, and transient voltage suppressors (TVS) can help mitigate unwanted EMI infiltration. Optimized PCB design with shorter traces, minimal loop areas, and proper isolation techniques further reduces EMI coupling. Protecting power supply lines through EMI-hardened regulators and isolated power domains prevents disruptions to critical components. To safeguard sensor interfaces, shielded cables, differential signal processing, and redundant sensing mechanisms should be employed to counter EMI-induced manipulation. Moreover, incorporating error-detection algorithms, watchdog timers, and fail-safe mechanisms ensures that EMI-induced faults are identified and mitigated in real-time. Conducting radiated susceptibility and conducted coupling tests under standardized conditions allows for a thorough assessment of BMS immunity and enhances design robustness. By integrating these countermeasures, BMS can be bolstered against EMI attacks, ensuring system reliability and operational safety in EVs and energy storage applications.

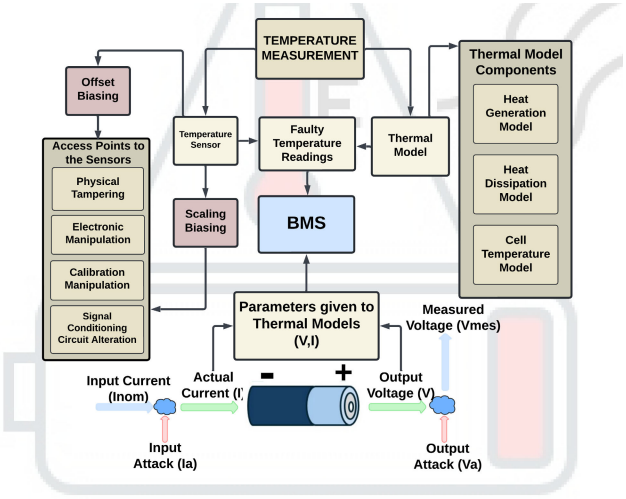


FIGURE 6. Illustration of temperature sensor manipulation and adversarial attacks: This Figure depicts how an adversary can manipulate temperature sensor readings to deceive the BMS. These adversarial attacks can lead to incorrect battery state estimations, potentially causing performance degradation, safety hazards, or enabling further malicious activities.

C. TEMPERATURE SENSING BIASING AND ADVERSARIAL ATTACKS

LIBs temperature is critical for ensuring the safety, performance, and longevity of energy storage systems. The BMS plays a vital role in reliably monitoring and regulating various battery parameters, with temperature being one of the key measurements along with current and voltage [69]. Excessive temperature can lead to a cascade of safety hazards. For example, **thermal runaway** - a dangerous condition where the battery rapidly heats up, releasing flammable electrolytes and potentially causing fire or explosion. High temperatures can also degrade battery performance by reducing capacity, shortening lifespan, and causing permanent damage to the internal structure of battery cells. Therefore, accurate and

continuous temperature monitoring by the BMS ensures safe operation, optimal performance, and accurate SOH estimation. To prevent thermal runaway, the BMS can leverage temperature readings to trigger safety features such as cell balancing, current limiting, or system shutdown. It can also adjust charging and discharging rates based on temperature to optimize performance and lifespan. Finally, temperature is a key factor in estimating the remaining capacity and health of the battery, providing valuable insights into battery SOH.

Two basic approaches are commonly used to measure temperature within battery packs for mobility systems. The first method relies on physical temperature sensors embedded directly within the battery pack. For this purpose, thermistors are commonly used to measure the temperature of the battery pack. Thermistors - semiconductor-based sensors exhibit a change in resistance with temperature, and thermocouples generate a voltage proportional to the temperature difference between two junctions. The second method utilizes software-based thermal models that estimate battery temperature based on other measurable parameters. These models typically consist of three parts: a heat generation model that estimates heat produced within the battery cell based on factors like current flow and internal resistance; a heat dissipation model that considers how heat transfers to the surrounding environment; and a cell temperature model that combines these factors to estimate cell temperature over time. While thermal models offer a more comprehensive picture of temperature distribution throughout the battery pack, they rely on accurate sensor data for calibration. Despite their widespread deployment, these methods may only sometimes capture rapid temperature fluctuations [56].

An accurate and reliable temperature estimation within a BMS is critical for ensuring the safety and performance of lithium-ion batteries in electric vehicles and energy storage systems. However, the measurements used for temperature estimation can be compromised through various attack methods targeting either the temperature sensors or the thermal models used for temperature estimation, as shown in Figure 6.

One such attack method is temperature sensor biasing, which involves artificially shifting the sensor readings. This can be achieved through physical tampering, where an external heat source elevates the reported temperature, or through electronic manipulation, where an attacker intercepts and modifies sensor data transmitted digitally between the sensor and the BMS. Another form of biasing is scaling bias, which multiplies the sensor readings by a factor. Attackers can achieve this by manipulating the calibration factor stored in the BMS memory during sensor initialization or by altering the signal conditioning circuitry responsible for amplifying or filtering the sensor signal. These physical access attacks can be achieved by accessing the temperature sensor or the BMS.

While sensor biasing poses a significant threat, a more sophisticated attack strategy involves manipulating both the input current profile and the output voltage measurements to deceive the thermal model used by some BMS systems. This approach, known as an adversarial attack, exploits the inherent reliance of thermal models on these parameters for temperature estimation. The attacker first introduces an additional attack current that alters the actual input current experienced by the battery cell, disrupting the normal relationship between current and heat generation. To further complicate detection, the attacker simultaneously introduces a voltage attack on the output side of the battery, altering the measured voltage observed by the BMS. By manipulating current and voltage measurements, the attacker aims to create a scenario where the thermal model receives misleading data. Since thermal models rely on accurate current and voltage data to estimate heat generation and dissipation within the battery cell, these manipulations can lead to significant errors in the estimated temperature, potentially masking unsafe conditions or causing the BMS to take inappropriate actions based on the false temperature reading. This adversarial attack highlights the vulnerability of thermal models when used in isolation, underlining the importance of robust sensor measurements for accurate temperature estimation in battery management systems.

Detecting temperature sensing manipulation in large-scale systems presents several challenges that impact real-time monitoring and system reliability. Latency in detection is a significant concern, as temperature fluctuations can occur rapidly, and delays in recognizing abnormal readings may lead to severe consequences, such as thermal runaway in batteries. Additionally, false rates pose a challenge in distinguishing between genuine and attack-related anomalies, such as overheating due to environmental factors and deliberate manipulations by adversaries who craft subtle changes to bypass conventional anomaly detection mechanisms. Implementing sensor redundancy can help cross-verify readings, but correlating data from multiple sensors in real-time adds computational complexity and increases system overhead. Another challenge lies in adversarial attacks on thermal models, where attackers manipulate input parameters like current and voltage to deceive the system, making detection more difficult. Communication channel security is also critical, as attackers can exploit vulnerabilities in wireless transmissions through man-in-the-middle attacks, altering sensor data before it reaches the BMS. While encryption can protect data integrity, real-time verification mechanisms are necessary to detect inconsistencies. Integrating AI-based anomaly detection offers potential solutions, but adversaries can introduce adversarial inputs to mislead ML models, reducing their effectiveness. Finally, system-wide monitoring challenges arise in large-scale grid storage or EV fleets, where tracking temperature anomalies across thousands of cells in real time requires significant computational resources and a scalable architecture. Addressing these challenges requires a multi-layered approach, combining hardware-based security, encrypted communication, adaptive AI-driven anomaly detection systems, and cross-verification techniques

to ensure the reliability and security of BMS temperature monitoring systems.

Tamper-resistant temperature sensors, encrypted sensor communication, and redundant sensing mechanisms are essential to prevent direct manipulation of sensor data in BMS. Cross-verification techniques integrating multiple temperature sensors and comparing readings with software-based thermal models enhance anomaly detection and mitigate inconsistencies in reported and measured values. Secured calibration procedures with crypto-based authentication ensure attackers cannot manipulate stored sensor parameters. By incorporating these security measures, BMS can effectively counter cyber threats stemming from temperature sensor manipulations, ensuring accurate thermal monitoring and maintaining system safety in EVs and other energy storage applications.

D. JAMMING ATTACKS ON WIRELESS BMS (wBMS)

The wBMS are revolutionizing battery management system research by replacing complex wired connections with wireless connectivity, offering significant advantages for modern battery packs [70]. Simplified design and assembly by eliminating cumbersome cable harnesses are the main motives behind wBMS design. It leads to increased packaging flexibility and space savings in applications with limited room, such as electric vehicles and UAVs [71]. In addition, weight reduction due to wBMD can extend operation time and range of both EVs and UAVs. Furthermore, wBMS facilitates more manageable maintenance and scalability due to the inherent simplicity of wireless modules. These modules can be effortlessly installed, serviced, and replaced, making battery module installation and removal very fast. At the core of a wBMS lie the **battery cell controllers** (BCCs), tiny computers attached to each battery cell that accurately monitor voltage, current, temperature, and other crucial BMS parameters.

A central wireless communication hub collects data from all BCCs and relays it to the Battery Management Unit (BMU) - the brain of the system. By analyzing data from BCCs, the BMU assesses the overall health and performance of the battery pack, taking control of charging, discharging, and safety functions to ensure optimal operation. To guarantee reliable data exchange with minimal impact on battery life, wBMS technology leverages various low-power wireless protocols. Bluetooth low energy is popular due to its low power consumption and sufficient range for short-distance communication within a battery pack. Near Field Communication (NFC), although not widely used currently in wBMS, offers a secure communication option for localized data exchange over very short ranges. The key functions of a wBMS encompass accurate cell monitoring, which involves continuous cell-level voltage monitoring and temperature monitoring to identify anomalies and ensure balanced operation. Additionally, a wBMS estimates the State of Charge (SoC), providing valuable insights into the remaining battery capacity based on historical data and real-time readings. Cell balancing is another critical function, where the wBMS actively balances charge levels across all cells to maximize battery life and prevent overcharging of individual cells. To ensure the safety of BMS, the wBMS incorporates overcharge/discharge protection, temperature management, and fault detection mechanisms to safeguard the battery pack from potential damage. Furthermore, a wBMS records battery health data for diagnostics, maintenance scheduling, and performance optimization through data logging and analysis. The applications of wBMS technology are diverse and span various battery-powered systems.

In EVs, wBMS is crucial in managing large battery packs, ensuring safety, efficiency, and extended battery life. Drones and UAVs heavily rely on wBMS for weight reduction and efficient battery management to achieve extended flight times. Portable electronics like laptops and tablets can benefit from wBMS by improving battery performance and lifespan. Large battery banks used for renewable energy integration or backup power systems leverage the flexibility and scalability advantages offered by wBMS. As wireless technology continues to evolve and battery packs become increasingly complex, wBMS are poised to play an even greater role in the future. Areas of development include improved communication range and security, with ongoing research focused on extending range while maintaining low power consumption and implementing robust encryption. Advanced diagnostics and analytics through machine learning are expected to be key for optimizing battery performance and lifespan through predictive maintenance and anomaly detection. Developing universal communication protocols will streamline wBMS integration across different battery pack manufacturers. By providing real-time data and intelligent control, wBMS technology transforms battery management, paving the way for safer, more efficient, and reliable battery-powered systems.

The wBMS is vulnerable to jamming attacks. A successful jamming attack on wBMS can disrupt wireless communication between BCCs, sensors, and the BCU, as shown in Figure7. This can lead to a cascade of problems. The conductor (control unit) may experience data loss, lacking crucial information about battery health due to missing sensor readings. Even if some data gets through, jamming attacks typically distort it, causing misinterpretation and potentially leading to incorrect charging or discharging decisions that jeopardize safety. In severe cases, the jamming can be so overwhelming that the control unit entirely loses control, like a conductor losing their grip on the orchestra. The consequences of this communication breakdown are significant. Safety risks arise from inaccurate data or the inability to control charging/discharging, potentially causing cell damage or thermal runaway (battery fire). Reduced performance can occur due to imbalanced cells or the inability to optimize charging cycles. Faulty cell balancing, where some cells are overworked while others are barely

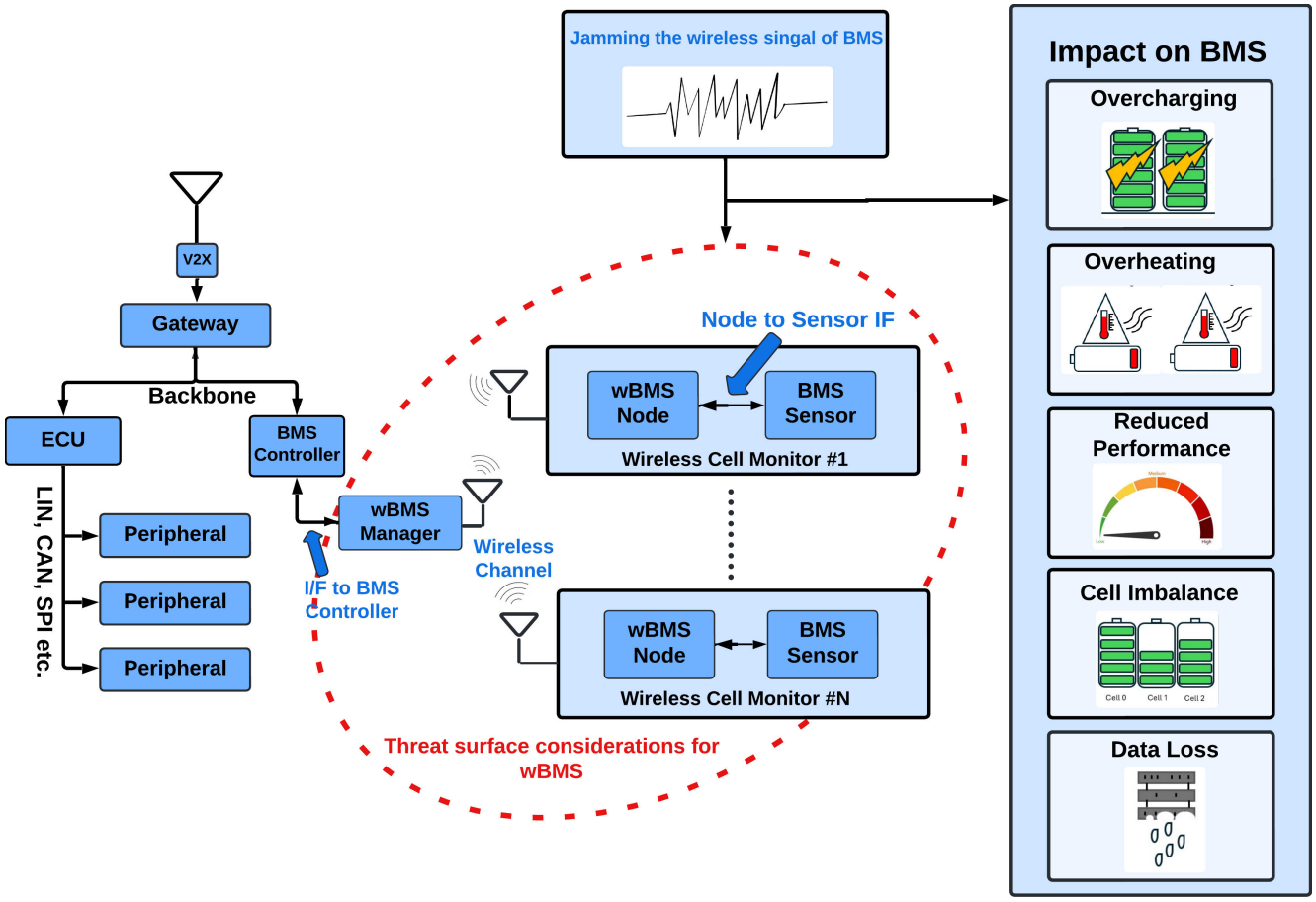


FIGURE 7. Illustration of Jamming Attack on wBMS: This diagram highlights how a jamming attack can disrupt wireless communication between battery cells and the wBMS. This interference can lead to data loss, communication failures, and potentially compromise the overall battery system performance and safety.

used, and increased wear and tear due to the lack of corrective actions further accelerate battery degradation. Understanding these jamming vulnerabilities is key to develope robust wBMS security measures. Wireless and radio communication security techniques like frequency hopping, encryption, and physical shielding can be employed to safeguard these systems against jamming attacks.

Implementing robust wireless security measures in wBMS ensures uninterrupted data exchange and enhances system reliability in EVs and energy storage applications. Techniques such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) mitigate signal interference by dynamically changing frequencies, making it challenging for attackers to sustain jamming attempts. Adaptive power control minimizes unnecessary transmission power, reducing susceptibility to interference while maintaining connectivity. Employing encrypted communication protocols ensures data integrity and prevents unauthorized signal manipulation. Implementing redundant multi-channel communication provides failover mechanisms, allowing data transmission through alternative paths in case of jamming attempts. Physical shielding and interference-resistant antennas enhance resilience against external electromagnetic disruptions. Additionally, AI-driven anomaly detection can monitor signal behavior in real-time, identifying and mitigating jamming attempts before they impact system performance. Collectively, these measures enable wBMS to maintain accurate battery management and enhance overall system reliability.

E. INTEGRATED CIRCUIT (IC)-COUNTERFEITING AND TAMPERING

BMS relies on an Integrated Circuits (IC) network to perform critical functions such as voltage monitoring, cell balancing, and safety control. However, these ICs are susceptible to exploitation through counterfeiting and tampering, introducing vulnerabilities into the entire BMS system. Counterfeiting involves the introduction of fake ICs that appear genuine during various stages of the BMS supply chain, including IC manufacturing and system manufacturing and integration. These counterfeit ICs can be degraded, recycled, remarked, or out-of-specification chips, leading to severe consequences for the BMS. Inaccurate measurements or malfunctions due to counterfeit ICs can impact battery lifespan and

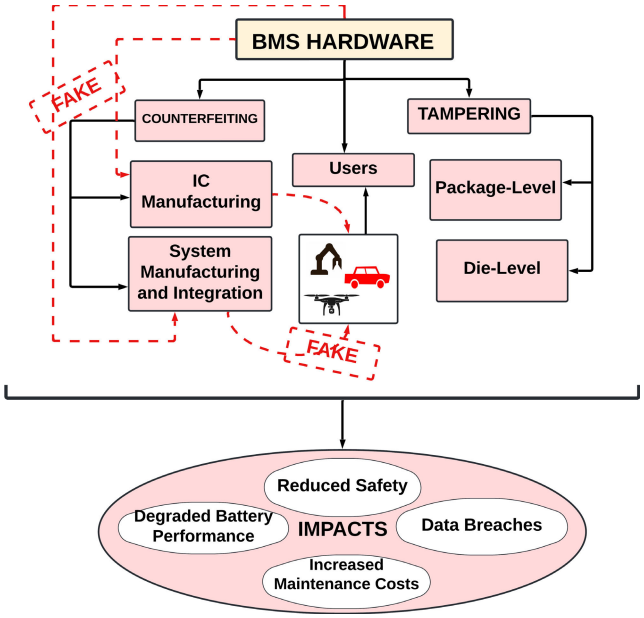


FIGURE 8. Illustration of IC Tampering for BMS.

performance. At the same time, lower-quality materials make these ICs more prone to failure, potentially damaging other BMS components. Furthermore, the BMS might only perform some of its intended functions due to the limitations of these degraded ICs, leading to functional downgrading.

Tampering with ICs involves physically altering existing ICs within the BMS and requires high technical expertise and physical access to the BMS hardware. There are two main methods of tampering: die-level tampering, which modifies the internal circuitry of the IC itself and requires highly sophisticated equipment. On the other hand, the package-level tampering alters the IC packaging to introduce malicious components or bypass security measures as shown in Figure 8. These malicious components, similar to "*hardware trojans*" found in counterfeit ICs, can act as silicon time bombs, waiting for specific conditions to activate and disrupt BMS operation by causing rapid battery draining, disabling safety features, or causing overheating. They can also create backdoors and hidden channels for attackers to steal sensitive data from the BMS, such as SoC or SoH. Tampering might also bypass security features built into the IC packaging, making the BMS more vulnerable to software attacks that exploit these vulnerabilities.

These hardware vulnerabilities can have a cascading effect on the entire BMS. A malfunctioning BMS due to compromised ICs can lead to safety risks such as overcharging, over-discharging, or thermal runaway, potentially causing fires or explosions. Inaccurate data and inefficient operation due to compromised ICs can significantly shorten battery life and reduce overall system performance. Frequent BMS failures or degraded battery performance necessitate more frequent replacements and repairs, leading to higher maintenance costs. Additionally, hardware Trojans acting as backdoors can allow attackers to steal sensitive information about the battery and the system it powers, leading to data breaches [38].

While most discussions around sensor tampering focus on intentional acts, accidental tampering is also significant. A well-documented example is a 2006 laptop battery recall by a major manufacturer due to the risk of overheating and fire caused by a faulty temperature sensor providing inaccurate readings, potentially leading to overcharging [72]. This highlights the importance of quality control in BMS design. Specific real-world examples of intentional sensor tampering in BMS are challenging to find publicly due to the sensitive nature of these incidents. However, some scenarios, such as tampering with a BMS sensor to gain insights into their battery design or performance, highlight the underlying dangers [43]. Likewise, counterfeiters might tamper with sensors in batteries to bypass safety features and make low-quality batteries appear functional, posing a significant fire risk to consumers or for military applications. Tampering with BMS sensors could be used to disable critical equipment powered by batteries or even cause explosions.

Trusted hardware sourcing is essential for strictly tracing components through blockchain or digital authentication, preventing counterfeit ICs from entering the system. Hardware integrity verification techniques, such as Physically Unclonable Functions (PUFs), chip fingerprinting, and side-channel analysis, can effectively detect unauthorized modifications. Tamper-resistant IC packaging and secure enclosures help prevent physical alterations, while AI-driven real-time anomaly detection can identify unexpected behavior caused by malicious modifications. Additionally, secure boot mechanisms and encrypted firmware updates safeguard against backdoor exploitation, ensuring firmware integrity. Regular hardware audits, IC testing, and compliance with industry standards are crucial for maintaining BMS security. By implementing these measures, BMS can be hardened against hardware-based threats, ensuring reliability, safety, and longevity in EVs and energy storage applications.

F. TIMESTAMP ATTACK ON BMS

A timestamp precisely records a specific event or data packet occurring within a system. It serves as a crucial element in establishing the chronological order of events, allowing systems to process and interpret data accurately. In the context of BMS, timestamps are vital for tracking the SOC, temperature, voltage, and other critical parameters. By ensuring that data is processed in the correct sequence, timestamps help maintain the system's reliability and efficiency. However, this seemingly straightforward element can become a target for attackers, leading to significant disruptions in BMS operations.

A timestamp attack involves altering the timestamps associated with data packets without modifying the underlying data. This manipulation can distort the perceived sequence of events, leading to a skewed view of system behavior, and for BMS, such attacks can be hazardous. For example,

during battery charging, an attacker might alter the timestamp associated with a SOC reading, misleading the BMS into thinking the battery is at a different charge level than it is. This can result in premature charging cycles, reduced battery lifespan, or unexpected system shutdowns. By tampering with the timestamps, attackers can deceive both the BMS and its corresponding digital twin [73], leading to inaccurate data interpretation and decision-making.

Several types of timestamp attacks can be used to target BMS. One trivial method involves intercepting and modifying data packets as they travel between system components, as illustrated in Figure 9. Attackers can alter the timestamps within these packets, disrupting the chronological order of events. Another approach is to exploit weaknesses in the communication protocols used by the BMS, allowing attackers to inject or modify timestamp information. By disrupting the synchronization between system clocks, attackers can create discrepancies in timestamps, leading to potential system confusion. Additionally, attackers may interpose between communicating parties, modifying data, including timestamps, without detection. Replay attacks, where previously recorded data packets are captured and retransmitted, can also create duplicate or out-of-order timestamps, further complicating the situation.

Timestamp manipulation attacks can have severe consequences for the security and reliability of BMS. By disrupting the chronological order of data, these attacks can hinder the system's ability to identify anomalies or detect faults accurately. This can impair predictive maintenance efforts and increase the risk of system failures. In electric vehicles, incorrect SOC information resulting from a timestamp attack can lead to range anxiety or, more critically, safety hazards if the vehicle underestimates its range. The altered data can also affect the digital twin used for advanced analytics and optimization, leading to inaccurate models and suboptimal decision-making. Incorrect data can result in safety hazards, such as battery fires or electric shocks, and economic losses due to premature battery replacements, reduced vehicle range, and increased charging times. Furthermore, successful attacks can expose vulnerabilities in the BMS and broader vehicle network, potentially allowing attackers to gain unauthorized access to other systems.

To summarize, timestamp manipulations pose a significant threat to the security and integrity of BMS. By altering timestamps, attackers can distort the system's perception of events, leading to incorrect data interpretation and potentially severe consequences. Understanding the mechanisms of these attacks and their impact on BMS is crucial for developing effective countermeasures. System designers and operators must prioritize securing communication channels, ensuring robust timestamp generation processes, and implementing checks for timestamp authenticity. As BMS evolves and becomes more complex, ongoing research and development are essential to staying ahead of emerging threats and safeguarding the systems that power modern EVs and energy storage solutions.

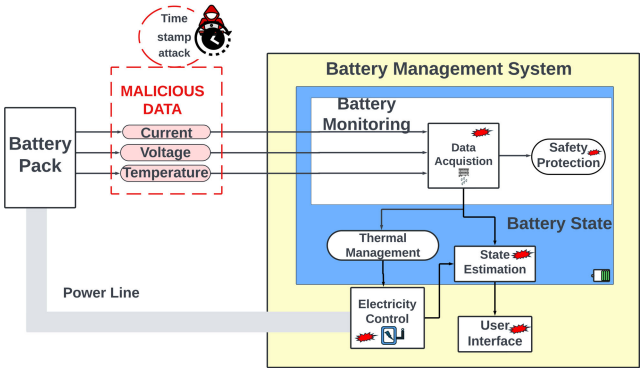


FIGURE 9. Illustration of timestamp attacks on BMS.

To mitigate timestamp attacks, time synchronization and tamper-resistant communication protocols are essential in BMS. Cryptographic timestamping techniques, such as hash-based message authentication codes (HMACs) or digital signatures, can verify timestamp authenticity and detect alterations. Secure clock synchronization mechanisms, including authenticated network time protocol (NTP) and encrypted precision time protocol (PTP), prevent attackers from injecting false timestamps. End-to-end encryption and secure communication protocols, like TLS or MQTT with security extensions, safeguard timestamp data from interception and modification. Multi-source timestamp verification enhances detection accuracy by cross-referencing time data from multiple trusted sources. Regular security audits, penetration testing, and firmware updates proactively address vulnerabilities in timestamp management. By integrating these measures, BMS can maintain data integrity, prevent unauthorized modifications, and enhance overall system reliability.

VII. FINDINGS AND PERSPECTIVES

Implementing robust cybersecurity measures in BMS is essential to safeguard it against potential cyberthreats and ensure the reliable operation of battery-powered systems. One fundamental approach is the application of encryption methods to protect data integrity and confidentiality. Encryption techniques such as Advanced Encryption Standard (AES) can secure communication between BMS components, preventing unauthorized access and tampering with critical data. In addition to encryption, deploying **Intrusion Detection Systems** (IDS) is vital for monitoring and identifying suspicious activities within the BMS. IDS can be designed to detect anomalies in communication patterns, data flows, and system behavior, enabling early detection and mitigation of potential cyberattacks. Moreover, best practices for secure BMS design include incorporating multi-layered security architectures that provide defense-in-depth, ensuring that if one layer is compromised, others remain intact to protect the system. Regular security assessments and updates, secure coding practices, and the implementation of robust authentication mechanisms are also crucial.

Employing hardware security modules (HSM) can enhance the security of cryptographic keys and sensitive information. Additionally, fostering a culture of cybersecurity awareness and training for personnel involved in BMS development and maintenance further strengthens the overall security posture. These measures collectively contribute to a resilient BMS capable of withstanding sophisticated cyber threats, ensuring safety and reliability in critical applications such as EVs and energy storage systems.

BMS for EV applications are particularly vulnerable to cyberattacks due to their high connectivity, mobility, and integration with multiple subsystems. Unlike stationary grid storage systems, EV BMS are exposed to wireless communication threats, remote exploits, and frequent user interactions, making them susceptible to man-in-the-middle attacks, jamming, malware injection, and sensor manipulation. The reliance on OTA updates and V2G interfaces further increases the risk of firmware tampering and data interception. Cyberattacks on EV BMS can also have immediate safety consequences, such as thermal runaway, vehicle immobilization, and battery degradation. In contrast, attacks on grid storage primarily impact energy availability and economic stability. These factors highlight the critical need for enhanced encryption, intrusion detection systems, and AI-driven anomaly detection to safeguard EV BMS against evolving cyber threats. However, all sectors require stringent security measures to mitigate threats such as firmware attacks, sensor manipulation, and malware infiltration.

Ensuring the cybersecurity of BMS requires adhering to stringent regulations and standards designed to protect against cyber threats and vulnerabilities. One of the pivotal standards in this domain is ISO/SAE 21434 [74], which provides a comprehensive framework for automotive cybersecurity engineering. The ISO/SAE 21434 outlines the requirements for managing cybersecurity risks throughout the lifecycle of automotive systems, from design and development to production, operation, and decommissioning. It emphasizes the importance of a risk-based approach, encouraging organizations to systematically identify, assess, and mitigate cybersecurity risks. For BMS specifically, compliance with ISO/SAE 21434 ensures that cybersecurity is integrated into the overall system design, addressing potential threats such as unauthorized access, data manipulation, and communication breaches. Additionally, standards such as ISO 26262 [75] for functional safety and IEC 62443 [76] for industrial automation and control systems offer guidelines that complement ISO/SAE 21434, further enhancing the cybersecurity posture of BMS. These standards advocate for secure coding, regular security assessments, and robust cryptographic measures. Regulatory frameworks, including the General Data Protection Regulation (GDPR), also play a crucial role by imposing strict data protection requirements, ensuring that personal and sensitive information managed by BMS is adequately safeguarded. Adhering to these regulations and standards mitigates cybersecurity risks and fosters trust among stakeholders by demonstrating a commitment to safety and security when deploying battery-powered systems. Collectively, these measures establish a robust foundation for the secure operation of BMS in critical applications, such as electric vehicles and energy storage systems, contributing to the overall resilience and reliability of modern technological infrastructures.

The increasing integration of BMS in EVs and energy storage solutions has drawn the attention of adversaries, leading to notable real-world cyberattacks. One prominent example is the EMI fault injection attack, where attackers use electromagnetic interference to induce faults in the BMS. This method can cause the system to misreport battery status, leading to potential overcharging or discharging, which poses significant safety risks. Mitigation strategies for such attacks include shielding sensitive components and implementing robust error detection and correction algorithms to identify and counteract erroneous data caused by EMI. Another notable incident involved malware injection into the BMS software, compromising its ability to accurately monitor and manage battery operations. Such attacks can result in unauthorized access and control, leading to unsafe operating conditions. To mitigate this threat, employing robust encryption techniques and secure boot mechanisms to verify the integrity of the software before execution is crucial. Regular software updates and patches also help close vulnerabilities that malware could exploit. Jamming attacks disrupt the communication signals within the BMS, representing another real-world threat. These attacks can obstruct the timely transmission of critical data, causing delayed or incorrect responses from the system. Mitigation measures include using frequency hopping spread spectrum (FHSS) to enhance the resilience of communication channels against jamming and implementing IDS that monitor and alert for abnormal communication patterns. These examples underscore the necessity of a multi-faceted cybersecurity approach to protect BMS from sophisticated cyber threats. By adopting comprehensive mitigation strategies, including physical protection, robust cryptographic measures, and advanced detection systems, stakeholders can significantly enhance the security and reliability of BMS in real-world applications.

Emerging technical advances, including AI and ML, are increasingly influencing the evolution of the BMS design, development, testing, and deployment processes. These technologies could significantly enhance monitoring, managing, and optimizing battery performance. AI and ML algorithms can analyze vast amounts of data generated by BMS in real-time, enabling predictive maintenance, fault detection, and accurate SoC and SoH estimations. By learning from historical and real-time data, these systems can predict potential failures before they occur, thereby improving the reliability and longevity of battery systems. However, integrating AI and ML into BMS also introduces new cybersecurity challenges. The reliance on data for training and decision-making makes these systems vulnerable to data poisoning attacks, where malicious data inputs can

TABLE 2. Potential cyberattacks and its consequences in battery management systems.

Typical Cyber Attacks	Entry Points	Consequences	Description
Malware Attack	- Software Bugs - Physical Connection	- Manipulated Sensor Data - Overcharging Batteries - Disrupted Thermal Management - Erroneous Control Actions - Unauthorized Access via Wireless Connectivity - Inaccurate Battery Management	- Malware can cause inaccurate BMS decisions - Unauthorized access and data manipulation
EMFI Attack	- IC input and Output pins - Wiring Harness - Power Supply Lines - Sensor Connections	- Misinterpreted Sensor Readings - Safety Shutdowns - Permanent Damage to BMS or Battery - Component Malfunction - Disrupted Power Flow	- Misinterpret sensor reading - Damage the BMS or battery, induce malfunctions and disrupt power flow
Temperature Attack	- Physical Tampering - Electronic Manipulation - Calibration Manipulator - Signal Conditioning and Circuit Alternator	- Thermal Runaway - Degraded Battery Performance - Permanent Damage to Battery Cells - Inaccurate State-of-Health (SOH) Estimation - Inappropriate BMS Actions - Masked Unsafe Conditions - Disrupted Normal Relationship	- Rapid heating of the battery, shorten lifespan, and damage internal structures. - Incorrect SOH estimation and hides potential hazards
Jamming Attack	- Network/Wireless Signal	- Data Loss - Distorted Data - Inability to control Charging/Discharging - Reduced Performance - Faulty Cell Balancing - Accelerated Battery Degradation	- Disrupts communication. - Prevents from managing charging cycles, reducing battery performance, - Increasing wear and tear, and accelerating battery degradation.
Counterfeiting Attack	- IC Manufacturing - System manufacturing and Integration	- Inefficient Operation - Higher Failure Rates - Functional Downgrading - Malicious Disruption - Data Breaches - Bypassed Security	- Inaccurate measurements and malfunctions and limiting its functionality. - Malicious components can rapidly drain the battery, create backdoors for data theft, and increase vulnerability to software attacks.
Tampering Attack	- Package Level - Die Level	- Safety Risks - Reduced Battery Life - Higher Maintenance - Industrial Espionage - Consumer Risk - Military Threats	- Causes thermal runaway and shortening battery life. - More repairs, expose design secrets, bypass safety features, and disable critical equipment
Timestamp Attack	-Intercepting data packets -Exploiting communication protocol - Disrupting clock synchronization - Replay attacks	-Disrupted chronological -system failures -Range anxiety in EVs - Exposed vulnerabilities in BMS and network - Inaccurate data for digital twin	- Altering timestamps of data packets without modifying the data itself - Attackers can cause various issues like incorrect SOC readings, leading to safety risks and economic losses.

corrupt the learning process, leading to incorrect predictions and actions. Moreover, adversarial attacks can deceive AI models by subtly altering input data, causing the system to misinterpret critical information. To mitigate these risks, robust data validation and anomaly detection mechanisms must be implemented to identify and filter out malicious

inputs. Secure model training practices, such as federated learning, can also enhance the resilience of AI models by distributing the learning process across multiple devices without sharing raw data, thus reducing the risk of data breaches. Additionally, the complexity of AI and ML algorithms necessitates comprehensive testing and validation to ensure they perform reliably under diverse conditions, including potential cyber threats. Incorporating explainability and transparency into AI models can help understand their decision-making processes, making identifying and rectifying vulnerabilities easier. As AI and ML continue to revolutionize BMS technology, a balanced approach that leverages their capabilities while addressing cybersecurity concerns is crucial for the safe and effective deployment of these advanced systems.

Various real-world incidents have highlighted the vulnerabilities of BMS. For a real-world instance, security flaws in Tesla's OTA updates and the Nissan Leaf's telematics system exposed vehicles to remote BMS manipulation. At the same time, large-scale grid storage fires in South Korea demonstrated how cyber threats or system malfunctions can trigger thermal runaway and explosions. Jeep Cherokee's CAN Bus hack and a Chinese EV fleet cyberattack revealed how attackers could alter SOC/SOH data, disrupt charging cycles, and immobilize vehicles. Cybercriminals have also targeted industrial energy storage systems with ransomware attacks, while IoT vulnerabilities in solar battery storage have led to false sensor data injection and system failures. These incidents underscore the urgent need for robust security measures such as encryption, authentication protocols, anomaly detection, intrusion detection systems, and secure firmware updates. The safety and mitigation strategies proposed in this paper effectively address these threats, enhancing BMS resilience and cybersecurity across critical applications.

Our analysis of cyberattacks targeting BMS identified various attack vectors and their potential consequences. We categorized these attacks based on their type, entry points, and impacts. Shown in Table 2 is a brief summary of these findings, revealing that attacks can exploit software, hardware, and communication vulnerabilities to manipulate sensor data, disrupt system operations, and compromise battery safety. Consequences include reduced battery life, and performance degradation, safety hazards, and potential system failures. These findings underscore the critical need for robust security measures to protect BMS from cyber threats.

VIII. CONCLUSION

The increasing complexity and connectivity of BMS are expanding their vulnerability to various attacks, including malware, EMI, sensor data manipulation, fault injection, and wireless jamming. These security threats can damage battery performance, accelerate degradation, and pose safety risks such as thermal runaway. Robust cybersecurity measures become crucial as BMS technology evolves with wireless capabilities and advanced analytics. Future advancements in BMS security should focus on implementing advanced encryption and authentication protocols to ensure data integrity and control access. Additionally, developing sophisticated anomaly detection algorithms for real-time threat mitigation and enhancing resilience against EMI and other interferences through improved shielding and fault-tolerant designs are essential. Critical steps include standardizing security protocols across the industry and integrating cybersecurity measures throughout the BMS lifecycle, from hardware selection to software development. This approach ensures secure and reliable operation of BMS in vital applications, such as electric vehicles, renewable energy storage, and beyond. Continuous research and collaboration among industry, academia, and cybersecurity experts are imperative to address emerging threats and adaptively safeguard BMS against evolving cyber threats.

REFERENCES

[1] H. Gabbar, A. Othman, and M. Abdussami, "Review of battery management systems (BMS) developand industrial standards," *Technologies*, vol. 9, no. 2, p. 28, Apr. 2021.
[2] P. Padwal, "Battery management system market size & share report-2030," SNS Insider Pvt Ltd, Austin, TX, USA, Feb. 2024.
[3] *Powering the Present and Future With Battery Management Systems*, Bosch, Gerlingen, Germany, 2024.
[4] *Denso Develops Next-generation Battery Management System for Electric Vehicles*, DENSO Corp., Kariya, Aichi, Japan, 2020.
[5] *Battery Management*, C. Engineering, Palmdale, CA, USA, 2024.
[6] *Battery Management System (bms) Market Worth $24.7 Billion By 2030 | Cagr: 18.3%*, Grand View Res., San Francisco, CA, USA, 2024.
[7] *China Ahead in Delivering Affordable Electric Mobility*, S. Global, London, U.K., 2024.
[8] *Carbon Footprint: How To Comply With Battery Regulation*, CIC energiGUNE, Alava, Spain, 2024.
[9] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2018, pp. 934–938.
[10] W. Liu, T. Placke, and K. T. Chau, "Overview of batteries and battery management for electric vehicles," *Energy Rep.*, vol. 8, pp. 4058–4084, Nov. 2022.
[11] Q. Lin, J. Wang, R. Xiong, W. Shen, and H. He, "Towards a smarter battery management system: A critical review on optimal charging methods of lithium ion batteries," *Energy*, vol. 183, pp. 220–234, Sep. 2019.
[12] Y. Zhao, O. Pohl, A. I. Bhatt, G. E. Collis, P. J. Mahon, T. Rüther, and A. F. Hollenkamp, "A review on battery market trends, second-life reuse, and recycling," *Sustain. Chem.*, vol. 2, no. 1, pp. 167–205, Mar. 2021.
[13] N. Tudoroiu, M. Zaheeruddin, R.-E. Tudoroiu, M. S. Radu, and H. Chammas, "Investigations on using intelligent learning techniques for anomaly detection and diagnosis in sensors signals in li-ion battery—Case study," *Inventions*, vol. 8, no. 3, p. 74, May 2023.
[14] C. Shell, J. Henderson, H. Verra, and J. Dyer, "Implementation of a wireless battery management system (WBMS)," in *IEEE Int. Instrum. Meas. Technol. Conf. (I2MTC) Proc.*, May 2015, pp. 1954–1959.
[15] V. Mali, R. Saxena, K. Kumar, A. Kalam, and B. Tripathi, "Review on battery thermal management systems for energy-efficient electric vehicles," *Renew. Sustain. Energy Rev.*, vol. 151, Nov. 2021, Art. no. 111611.
[16] A. Nath and B. Rajpathak, "Analysis of cell balancing techniques in BMS for electric vehicle," in *Proc. Int. Conf. Intell. Controller Comput. Smart Power (ICICCSP)*, Jul. 2022, pp. 1–6.
[17] N. Khan, C. A. Ooi, A. Alturki, M. Amir, Shreasth, and T. Alharbi, "A critical review of battery cell balancing techniques, optimal design, converter topologies, and performance evaluation for optimizing storage system in electric vehicles," *Energy Rep.*, vol. 11, pp. 4999–5032, Jun. 2024.
[18] K. Bhaskar, A. Kumar, J. Bunce, J. Pressman, N. Burkell, N. Miller, and C. D. Rahn, "State of charge and state of health estimation in large lithium-ion battery packs," in *Proc. Amer. Control Conf. (ACC)*, May 2023, pp. 3075–3080.

[19] D. Vaish and R. R. Nair, "Robust battery management system for electric vehicles," in *Proc. Int. Conf. Comput., Electron. Electr. Eng. Appl. (IC2E)*, Jun. 2023, pp. 1–6.

[20] S. Venkatakrishnan, V. Sudhan V. M., S. Kandappan S., S. Vishwanath, S. Saravanan, and P. Pandiyan, "Battery thermal management system," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 877–882.

[21] F. Baronti, G. Fantechi, E. Leonardi, R. Roncella, and R. Saletti, "Hierarchical platform for monitoring, managing and charge balancing of LiPo batteries," in *Proc. IEEE Vehicle Power Propuls. Conf.*, Sep. 2011, pp. 1–6.

[22] L. O. Avila, M. L. Errecalde, F. M. Serra, and E. C. Martinez, "State of charge monitoring of li-ion batteries for electric vehicles using GP filtering," *J. Energy Storage*, vol. 25, Oct. 2019, Art. no. 100837.

[23] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, no. 11, p. 3931, May 2022.

[24] S.-J. Park, Y.-W. Song, B.-S. Kang, W.-J. Kim, Y.-J. Choi, C. Kim, and Y.-S. Hong, "Depth of discharge characteristics and control strategy to optimize electric vehicle battery life," *J. Energy Storage*, vol. 59, Mar. 2023, Art. no. 106477.

[25] M. Uzair, G. Abbas, and S. Hosain, "Characteristics of battery management systems of electric vehicles with consideration of the active and passive cell balancing process," *World Electric Vehicle J.*, vol. 12, no. 3, p. 120, Aug. 2021.

[26] R. D. McKerracher, J. Guzman-Guemez, R. G. A. Wills, S. M. Sharkh, and D. Kramer, "Advances in prevention of thermal runaway in lithium-Ion batteries," *Adv. Energy Sustainability Res.*, vol. 2, no. 5, Mar. 2021, Art. no. 2000059.

[27] X. Kong, Y. Zheng, M. Ouyang, X. Li, L. Lu, J. Li, and Z. Zhang, "Signal synchronization for massive data storage in modular battery management system with controller area network," *Appl. Energy*, vol. 197, pp. 52–62, Jul. 2017.

[28] B. Ragchaa, L. Wu, and X. Zhang, "A design of fault-tolerant battery monitoring IC for electric vehicles complying with ISO 26262," *IEEE Open J. Circuits Syst.*, vol. 5, pp. 166–177, 2024.

[29] K. W. See, G. Wang, Y. Zhang, Y. Wang, L. Meng, X. Gu, N. Zhang, K. C. Lim, L. Zhao, and B. Xie, "Critical review and functional safety of a battery management system for large-scale lithium-ion battery pack technologies," *Int. J. Coal Sci. Technol.*, vol. 9, no. 1, p. 36, Dec. 2022.

[30] V. Gupta, H. Priyadarshi, V. Goyal, K. Singh, A. Shrivastava, and J. Akhtar, "BMS-driven onsite insolation charging infrastructure for electric vehicles," *AIP Conf. Proc.*, vol. 2294, Dec. 2020, Art. no. 040006.

[31] V. Vaideeswaran, S. Bhuvanesh, and M. Devasena, "Battery management systems for electric vehicles using lithium ion batteries," *Innov. Power Adv. Comput. Technol. (i-PACT)*, vol. 11, pp. 1–9, Mar. 2019.

[32] R. Gozdur, T. Przerywacz, and D. Bogda ski, "Low power modular battery management system with a wireless communication interface," *Energies*, vol. 14, no. 19, p. 6320, Oct. 2021.

[33] A. Reindl, V. Schneider, H. Meier, and M. Niemetz, "Software update of a decentralized, intelligent battery management system based on multi-microcomputers," in *Proc. 2 Symp. Elektronik und Systemintegration ESI 2020, 'Intelligente Systeme und ihre Komponenten: Forschung und industrielle Anwendung'*, 2020, pp. 8–19.

[34] B. G. Carkhuff, P. A. Demirev, and R. Srinivasan, "Impedance-based battery management system for safety monitoring of lithium-ion batteries," *IEEE Trans. Ind. Electron.*, vol. 65, no. 8, pp. 6497–6504, Aug. 2018.

[35] M. Cheah and R. Stoker, "Cybersecurity of battery management systems," *HM TR Ser.*, vol. 10, no. 3, p. 8, 2019.

[36] G. Krishna, R. Singh, A. Gehlot, S. V. Akram, N. Priyadarshi, and B. Twala, "Digital technology implementation in battery-management systems for sustainable energy storage: Review, challenges, and recommendations," *Electronics*, vol. 11, no. 17, p. 2695, Aug. 2022.

[37] Q. Lu, X. Xie, A. K. Parlikad, and J. M. Schooling, "Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance," *Autom. Construction*, vol. 118, Oct. 2020, Art. no. 103277.

[38] A. B. Lopez, K. Vatanparvar, A. P. D. Nath, S. Yang, S. Bhunia, and M. A. A. Faruque, "A security perspective on battery systems of the Internet of Things," *J. Hardw. Syst. Secur.*, vol. 1, no. 2, pp. 188–199, Jun. 2017.

[39] G. Bere, J. J. Ochoa, T. Kim, and I. R. Aenugu, "Blockchain-based firmware security check and recovery for battery management systems," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2020, pp. 262–266.

[40] N. Mishra, S. Hafizul Islam, and S. Zeadally, "A survey on security and cryptographic perspective of industrial-Internet-of-Things," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101037.

[41] P. Labbé, A. Ghanmi, and M. Abdelazez, "Current and future hypersonic threats, scenarios and defence technologies for the security of Canada," Defence Res. Develop. Canada, Ottawa, ON, Canada, Sci. Rep. DRDC-RDDC-2022-R046, Mar. 2022.

[42] M. Pasetti, P. Ferrari, P. Bellagente, E. Sisinni, A. O. de Sá, C. B. D. Prado, R. P. David, and R. C. S. Machado, "Artificial neural network-based stealth attack on battery energy storage systems," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5310–5321, Nov. 2021.

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

[44] G. Krishna, R. Singh, A. Gehlot, N. Yamsani, S. Kathuria, and S. V. Akram, "Enhancing the cyber-security of battery management systems for energy storage," in *Proc. IEEE World Conf. Appl. Intell. Comput. (AIC)*, Jul. 2023, pp. 959–964.

[45] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," 2017, *arXiv:1711.04822*.

[46] R. R. Kumar, C. Bharatiraja, K. Udhayakumar, S. Devakirubakaran, K. S. Sekar, and L. Mihet-Popa, "Advances in batteries, battery modeling, battery management system, battery thermal management, SOC, SOH, and charge/discharge characteristics in EV applications," *IEEE Access*, vol. 11, pp. 105761–105809, 2023.

[47] M. Manas, R. Yadav, and R. K. Dubey, "Designing a battery management system for electric vehicles: A congregated approach," *J. Energy Storage*, vol. 74, Dec. 2023, Art. no. 109439.

[48] S. Lee and A. Kim, "Online real-time SOH prediction and anomaly detection under dynamic load conditions and nonstandard practice," *IEEE Access*, vol. 11, pp. 75912–75928, 2023.

[49] M. Lelie, T. Braun, M. Knips, H. Nordmann, F. Ringbeck, H. Zappen, and D. U. Sauer, "Battery management system hardware concepts: An overview," *Appl. Sci.*, vol. 8, no. 4, p. 534, Mar. 2018.

[50] T. Zheng, "Fault diagnosis of overcharge and overdischarge of lithium ion batteries," *Chem. Eng. Trans.*, vol. 71, pp. 1453–1458, Dec. 2018.

[51] K. Xie, L. Han, K. Ma, F. Wang, B. Wang, J. Chen, and Y. Gao, "A method for measuring and evaluating the fault response performance of battery management system," *Energy Rep.*, vol. 8, pp. 639–649, Feb. 2022.

[52] M. Schmid, H.-G. Kneidinger, and C. Endisch, "Data-driven fault diagnosis in battery systems through cross-cell monitoring," *IEEE Sensors J.*, vol. 21, no. 2, pp. 1829–1837, Jan. 2021.

[53] C. Zhen, Z. Chen, and D. Huanz, "A novel sensor fault diagnosis method for lithium-ion battery system using hybrid system modeling," in *Proc. Condition Monitor. Diagnosis (CMD)*, Sep. 2018, pp. 1–5.

[54] Y. Cheng, M. D'Arpino, and G. Rizzoni, "Fault diagnosis in lithium-ion battery of hybrid electric aircraft based on structural analysis," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2022, pp. 997–1004.

[55] A. A. Fedorova, D. V. Anishchenko, E. V. Beletskii, A. Y. Kalnin, and O. V. Levin, "Modeling of the overcharge behavior of lithium-ion battery cells protected by a voltage-switchable resistive polymer layer," *J. Power Sources*, vol. 510, Oct. 2021, Art. no. 230392.

[56] S. Kumar Padisala, S. Dhananjay Vyas, and S. Dey, "Exploring adversarial threat models in cyber physical battery systems," 2024, *arXiv:2401.13801*.

[57] T.-W. Sun and T.-H. Tsai, "A battery management system using interleaved pulse charging with charge and temperature balancing based on NARX network," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 4, pp. 1811–1819, Apr. 2022.

[58] L. Crocetti, R. Di Rienzo, A. Verani, F. Baronti, R. Roncella, and R. Saletti, "A novel and robust security approach for authentication, integrity, and confidentiality of lithium-ion battery management systems," in *Proc. IEEE 3rd Int. Conf. Ind. Electron. Sustain. Energy Syst. (IESES)*, Jul. 2023, pp. 1–6.

[59] S. Dey, S. Mohon, P. Pisu, and B. Ayalew, "Sensor fault detection, isolation, and estimation in lithium-ion batteries," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 6, pp. 2141–2149, Nov. 2016.

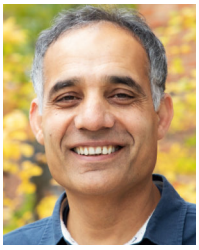
[60] O. Aiello, "Electromagnetic susceptibility of battery management systems' ICs for electric vehicles: Experimental study," *Electronics*, vol. 9, no. 3, p. 510, Mar. 2020.

[61] Z. Wang, G. Zhang, X. Zhao, W. Hou, R. Feng, and H. Xu, "Fault detection system of charging pile based on embedded device," in *Proc. 8th Asia Conf. Power Electr. Eng. (ACPEE)*, Apr. 2023, pp. 2629–2633.
[62] R. Zhang, J. Wu, R. Wang, R. Yan, Y. Zhu, and X. He, "A novel battery management system architecture based on an isolated power/data multiplexing transmission bus," *IEEE Trans. Ind. Electron.*, vol. 66, no. 8, pp. 5979–5991, Aug. 2019.
[63] T. Wu, D. Zhou, L. Du, and S. Wang, "Fault template attack based on fault probability," *IEEE Access*, vol. 11, pp. 71705–71713, 2023.
[64] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2020, pp. 98–103.
[65] B. Kiamanesh, A. Behravan, and R. Obermaisser, "Realistic simulation of sensor/actuator faults for a dependability evaluation of demand-controlled ventilation and heating systems," *Energies*, vol. 15, no. 8, p. 2878, Apr. 2022.
[66] O. Aiello, P. S. Crovetti, and F. Fiori, "Susceptibility to EMI of a battery management system IC for electric vehicles," in *Proc. IEEE Int. Symp. Electromagn. Compat. (EMC)*, Aug. 2015, pp. 749–754.
[67] H. Liao, "Electromagnetic fault injection on two microcontrollers: Methodology, fault model, attack and countermeasures," M.S. thesis, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, Feb. 2020.
[68] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz, "Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller," in *Proc. Workshop Fault Diagnosis Tolerance Cryptography*, Aug. 2013, pp. 77–88.
[69] M. Y. A. Shdaifat, R. Zulkifli, K. Sopian, and A. A. Salih, "Basics, properties, and thermal issues of EV battery and battery thermal management systems: Comprehensive review," *Proc. Inst. Mech. Engineers, D, J. Automobile Eng.*, vol. 237, nos. 2–3, pp. 295–311, Feb. 2023.
[70] P. Gu and R. M. Gerdes, "Linear-quadratic game theoretic analysis for securing battery management power converter systems," in *Proc. 2nd ACM Workshop Automot. Aerial Vehicle Secur.*, Mar. 2020, pp. 15–22.
[71] F. Tlili, L. C. Fourati, S. Ayed, and B. Ouni, "Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures," *Ad Hoc Netw.*, vol. 129, Apr. 2022, Art. no. 102805.
[72] *How Dell Laptop Batteries Work: Battery Fires*, HowStuffWorks, Atlanta, GA, USA, 2024.
[73] M. Pooyandeh and I. Sohn, "A time-stamp attack on digital twin-based lithium-ion battery monitoring for electric vehicles," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2024, pp. 499–502.
[74] C. Schmittner, G. Griessnig, and Z. Ma, "Status of the development of ISO/SAE 21434," in *Systems, Software Services Process Improvemen*, X. Larrucea, I. Santamaria, R. V. O'Connor, and R. Messnarz, Eds., Cham, Switzerland: Springer, 2018, pp. 504–513.
[75] R. Palin, D. Ward, I. Habli, and R. Rivett, *ISO 26262 Safety Cases: Compliance and Assurance*, Standard ISO 26262, 2011, p. 12.
[76] P. M. C. Hazell, "Integrating IEC 62443 cyber security with existing industrial process and functional safety management systems," *Eng. Technol. Reference*, vol. 1, no. 1, pp. 1–23, Feb. 2017.

SHRAVAN MURLIDHARAN received the B.Tech. degree in electronics and communication engineering from Chennai, India. He is currently pursuing the M.S.E. degree in electrical engineering with the University of Michigan-Dearborn. His research interests include automotive systems, autonomous vehicles, vehicle electrification, and cybersecurity, with an emphasis on developing innovative solutions to enhance the efficiency and safety of next-generation mobility systems. His work spans battery management system (BMS), advanced driver assistance systems (ADAS), and secure communication frameworks for electric, connected, and autonomous vehicles, contributing to sustainable and intelligent transportation technologies.

VARSHA RAVULAKOLE received the B.Tech. degree in electronics and communication engineering in Hyderabad, India. She is currently pursuing the M.S.E. degree in electrical engineering with the University of Michigan-Dearborn. Her research interests include automotive safety systems, vehicle cybersecurity, and battery management system (BMS). She is particularly interested in developing robust solutions to enhance the safety and security of connected and electrified vehicles. Her work addresses critical challenges in vehicle cybersecurity, energy management, and system reliability, contributing to the advancement of secure and sustainable transportation technologies.

JYOTHI KARNATI received the B.Tech. degree in electrical and electronics engineering in Vijayawada, India. She is currently pursuing the M.S.E. degree in computer engineering with the University of Michigan-Dearborn. Her research interests include automotive Ethernet and battery management system (BMS), with an emphasis on enhancing connectivity and energy efficiency in modern vehicles. She is particularly interested in the design and optimization of communication networks for automotive applications and the development of advanced battery management solutions. Her work aims to contribute to the evolution of intelligent and sustainable transportation systems.



HAFIZ MALIK (Senior Member, IEEE) is currently a Professor of electrical and computer engineering (ECE) with the University of Michigan-Dearborn. He has published more than 180 articles in leading peer-reviewed journals, conferences, and workshops. His research interests include deepfakes, automotive cybersecurity, cyber-physical system security, sensor security, multimedia forensics, steganography/steganalysis, information hiding, pattern recognition, and information fusion is funded by the National Science Foundation, National Academies, Ford Motor Company, Marelli, Inc. N.A., and other agencies. He is also a Founding Member and the Chief Operating Officer (COO) of the Global Foundation for Cyber Studies and Research, a Founding Member of the Cybersecurity Center for Research, Education, and Outreach at UM-Dearborn, and a member of the leadership circle for the Dearborn Artificial Intelligence Research Center at UM-Dearborn. He is also a member of the Scientific and Industrial Advisory Board (SIAB) of the National Center of Cyber Security Pakistan. He has been a member of the MCity Working Group on Cybersecurity, since 2015. He was a recipient of the UM-Dearborn Chancellor's Inclusive Excellence Fellows 2022, the UM-Dearborn 2022 Distinguished Research Award, and the College of Engineering and Computer Science 2020 Excellence in Research Award. He is the founder and CEO of Media Shield Inc.–a robust and reliable deepfake detection platform. Further information about his research can be found at http://www-personal.umd.umich.edu/ hafiz/.