INSPECT: Investigating Supply Chain and Cyber-Physical Security of Battery Systems

Tao Zhang, Shang Shi, Md Habibur Rahman, Nitin Varshney, Akshay Kulkarni, Farimah Farahmandi, and Mark Tehranipoor
Department of Electrical and Computer Engineering, University of Florida
Email: {tao.zhang, shang.shi, rahman.mdhabibur, nitinvarshney1, kulkarniakshay}@ufl.edu and {farimah, tehranipoor}@ece.ufl.edu

***Abstract*—Battery-operated applications have been ubiquitous all over the world ranging from power-intensive electric cars down to low-power smart terminals and embedded devices. Meanwhile, serious incidents around batteries such as swelling, fire, and explosion have been witnessed, which resulted in horribly huge financial and even life loss. People used to attribute such aftermaths to unintentional design mistakes or insufficient quality inspection of original battery manufacturers. However, this is not fair anymore today given the convoluted battery supply chain and the extended cyber-physical attack surface of battery management systems (BMS). In this paper, we will focus on the *authenticity* and *assurance* of prevalent (Li-ion) battery instances. We look into battery authenticity by modeling the contemporary battery supply chain and discussing practical concerns such as rewrapping and recycling in-depth at each stage. As for battery assurance, we consider emerging attack vectors that can compromise the confidentiality, integrity, and availability of the microelectronic BMS. Besides, real-world attack examples are highlighted to reflect the capabilities of advanced adversaries. Moreover, promising countermeasures regarding the detection and avoidance of threats on both battery authenticity and assurance are presented, such that researchers will gain insights into how the problem could be addressed/alleviated. We also provide our perspectives on the vulnerabilities of battery systems and their consequent impacts as well as our point of view on potential countermeasure techniques.**

***Index Terms*—Battery systems, cyber-physical security, supply chain security, counterfeit detection, perspective countermeasures.**

I. Introduction

Over the past decades, the battery market has been skyrocketing due to the proliferation of various industrial segments and applications ranging from electric vehicles (EVs) to consumer electronics. As depicted in Fig. 1, the battery market size in 2023 is $136B in total where Lithium-ion (Li-ion) batteries occupy around $70B which far exceeds their counterparts such as lead-acid and Zinc-air batteries [1], making them a market-dominating variant globally. The prosperity of Li-ion batteries can be attributed to features like high energy density, small size/weight, and long life span. Therefore, advanced applications significantly benefit from Li-ion batteries, which jointly and fundamentally revolutionize people's lifestyles and the world. The distributions of Li-ion market shares across applications are that EVs, consumer electronics, and energy storage serve as the primary driving power by making up 41.4%, 13.9%, and 9.9% of the entire Li-ion battery market in 2023, respectively [2]. Furthermore, as of today, it is universally acknowledged that the need for the aforementioned battery-operated applications is still rapidly growing, thus leading to the exponentially upward trend of the Li-ion battery market as presented in Fig. 1, i.e., from $70B today to the projected $257B in 2030.

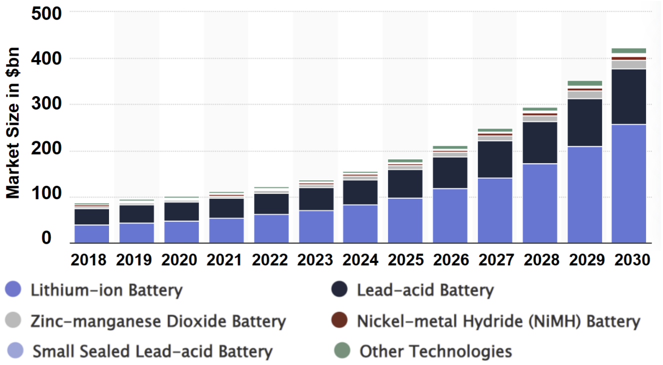


Fig. 1. The market share of each category of batteries and the growing trend [1]

Despite the promising market expansion, security/safety incidents around Li-ion batteries have been witnessed incessantly throughout the past years. The widespread applications exaggerate such concerns especially given that most of them (e.g., EVs and medical devices) are pretty sensitive to financial loss and even human life. Table I summarizes the incidents of significant aftermath in recent years chronologically. For instance, in 2012, there are quite a few police officers got seriously injured because of the explosion of batteries in their law enforcement equipment [3]. Besides, at least 26 users were burned by battery overheating, igniting, and explosion of Samsung Galaxy Note 7 incidents in 2016. The mandatory callback of such mainstream smartphones further results in a heavy revenue loss of more than $5 billion [4]. Additionally, Table I reflects other battery fire incidents, leading to tragedies including property damages [5, 6], emergency landing of flights [7], and people death/injury [8–10].

Intuitively, these unceasingly emerging incidents could stem from the immanent reliability issues of batteries which can be mostly attributed to original designers/manufacturers, e.g., inappropriate implementations and inability to withstand harsh conditions. Dangerous circumstances like fires and explosions are mainly caused by a phenomenon *thermal runaway*, i.e., the

TABLE I
RECENT SECURITY INCIDENTS AROUND LI-ION BATTERIES.

Incident	Aftermath	Year
Series of phone battery explosion [5]	Life threats and financial loss	2011
Police equipment battery explosion [3]	Officers seriously injured	2012
Counterfeit batteries in U.S DoD [12]	$2.6M revenue loss	2014
Hoverboards with counterfeit batteries [13]	$20M revenue loss	2016
Smartphone recall by explosive batteries [4]	$5B revenue loss	2016
Hoverboard battery fire [6]	2 houses burnt down	2017
Counterfeit batteries sale [14]	$23.8M revenue loss	2019
Flight cargo fire [7]	Plane forced into landing	2020
E-bike battery fire [8]	40 people injured in Manhattan	2022
Counterfeit batteries supplied to DLA [15]	Amount involved of $75,000	2022
Counterfeit battery fire [9]	House burnt down and 12 people hurt	2023
EV battery fire [10]	4125 EV combustion annually	2023

heat produced by battery exothermic reactions surpasses the heat dissipated into the surroundings [11] such that the heat can be accumulated to result in an exponential temperature surge. The root causes of thermal runaway are mechanical abuse, electric abuse, and thermal abuse, as explained below.

- **Mechanical Abuse:** Physical accidents like crashing or penetration can cause the deformation of the battery cell and tearing of the separator inside, which could create an internal short circuit and generate massive amounts of heat [11] to induce thermal runaway.
- **Electric Abuse:** Electric abuse is a result of electrical overloading operations like overcharging or short circuits. It could inspire the growth of the dendrite and the piercing of the separator [11], making the internal short circuit worse while accelerating the generation of the heat.
- **Thermal Abuse:** Due to the external overheating and collapse of the separator by electric abuse or mechanical abuse, the battery would exceed the temperature threshold and enter the stage of thermal runaway [11].

Although almost all Li-ion battery manufacturers have been striving to make their products more reliable to mitigate inherent quality concerns like thermal runaway [16], this falls short by a long way in ensuring the safety of batteries and battery-operated devices because of the oversights into two critical facts, i.e., battery (system) *authenticity* and *assurance*. Specifically, *authenticity* refers to the battery being genuine and legitimate, which involves determining whether a given battery is an authentic and authorized product. As tabulated in Table I, counterfeit batteries are profitable and ubiquitous given the complicated battery supply chain. Counterfeiters can reclaim used batteries from discarded systems and sell them as new components, posing safety risks and resulting in a reduced lifetime. For example, there are numerous counterfeit batteries identified in the U.S. Department of Defense (DoD) applications, inducing a loss of `$2.6M` [12]. Furthermore, counterfeit battery sales have been seen in a variety of applications like hoverboards [13], EVs [10], and other defense infrastructure [15], causing financial loss of up to `$23.8M` in a single reported case [14]. Note that besides the *authenticity* concerns induced by counterfeit battery cells and supply chain attacks, *assurance* of a battery management system (BMS) [17] could be compromised at the same time, making the issues even more complicated. A typical BMS is an attached microelectronic device to enable precise battery monitoring and timely status/data management [17]. As such, batteries can interact with other components and upper applications through in-system or wireless connectivity. In other words, a BMS-enabled battery can be considered as a *cyber-physical system* (CPS) where its *assurance* stands for preserving three properties of utmost importance, i.e., *confidentiality*, *integrity*, and *availability*. There could be numerous attack vectors like denial-of-service (DoS) [18] and hardware tampering [19], violating these properties of battery systems to actively yield aftermaths in Table I.

Given the aforementioned concerns around battery *authenticity* and *assurance*, there have been detection and avoidance solutions to mitigate them. However, unfortunately, a silver bullet is not available to address the concerns completely. For instance, visual and X-ray inspection of the target battery is a common method to distinguish counterfeit instances from a batch [20]. However, such techniques can hardly cope with meticulous camouflaging [21], allowing for the escape of counterfeit batteries into open markets. As for the countermeasures against cyber attacks on batteries, a general approach refers to behavior-based detection [22] where the run-time behaviors of BMS-related components, e.g., network traffic, system status, and data would be compared to a golden (attack-free) reference to yield the residual statistics. The residual signals stand for the deviations of run-time behaviors from their references, which can indicate potential intrusions. The behavior-based detection is comprehensive but the required data volume can be prohibitively large [23], making it an inappropriate fit for complicated applications such as EVs and power grids. In addition to cyber attack vectors, physical hardware, i.e., microelectronic devices themselves in BMS, can serve as the victim of compromise. Backdoors or hardware Trojans [24, 25] could be implanted into them such that the entire BMS can become vulnerable against assurance violations [26]. However, Trojan detection [27] remains an open challenge in the hardware security domain as of today. Moreover, note that such BMS hardware trust problems can not only be caused by conventional adversaries in the semiconductor supply chain but also by battery counterfeiters who intend to replace the benign BMS with malicious devices, which require more comprehensive investigations and advanced countermeasures [28–31].

With the aforementioned problem statements and limitations in mind, battery security issues (authenticity and assurance) call for more deliberate considerations and examinations in the landscape of both problems and countermeasures. Therefore, in this paper, we aim to give a comprehensive overview of battery security including counterfeit batteries, cyber-physical threats on battery systems, and existing/possible countermeasures. The contributions of the paper are summarized below:

- We investigate the supply chain model of Li-ion batteries to identify the main actors and stages. Also, the battery authenticity issues are analyzed at each phase of the supply chain, providing readers with an in-depth understanding of why and how counterfeit batteries could be introduced in final products.
- We analytically present the threat model on in-field battery systems by covering the assurance concerns with respect to confidentiality, integrity, and availability. The

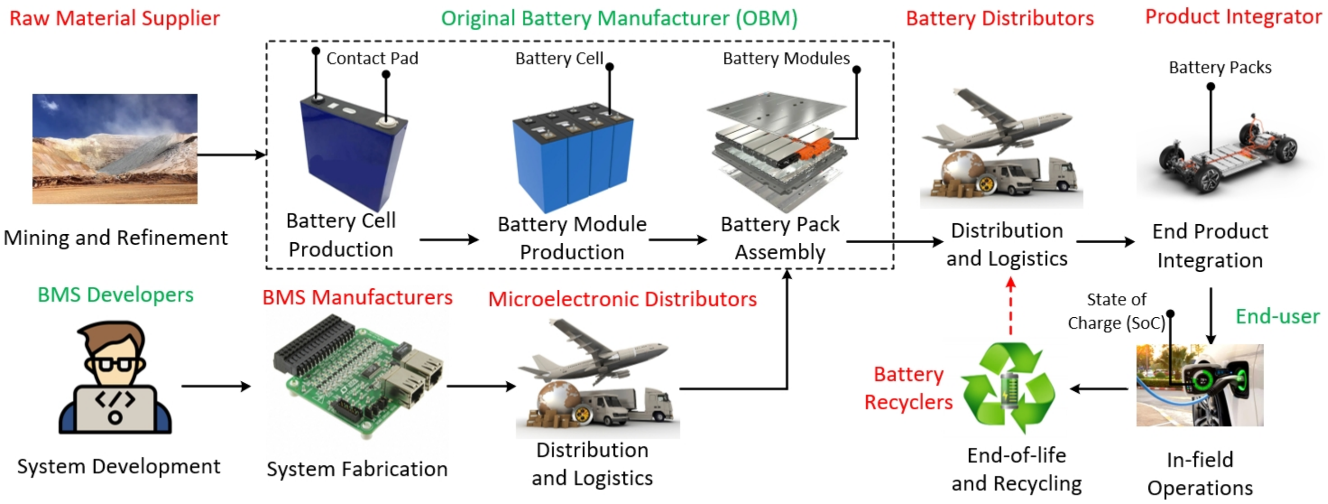


Fig. 2. Li-ion battery supply chain model with notations of benign entities (green) and potential adversaries (red) in our threat model.

attack surface from network to underlying hardware is considered along with real-world examples illustrating how adversaries can exploit these vulnerabilities.

- We review existing detection and avoidance methodologies that aim at mitigating authenticity and assurance issues of battery systems. Moreover, perspectives on promising countermeasures such as battery physical unclonable function (PUF), blockchain technology for battery supply chain management, and zero-trust architecture are discussed.

The rest of this paper is organized as follows. Section II presents the supply chain model of battery systems while the vulnerabilities at each stage are discussed. Section III details the cyber-physical security threats from software to the hardware of BMS. Section IV reviews the existing solutions enhancing battery system authenticity and assurance while Section V presents perspective methodologies in our mind that could help address or mitigate the threats. Finally, Section VI concludes this paper.

II. Battery Supply Chain Security Issues

Due to their widespread usage, the Li-ion battery supply chain is becoming increasingly convoluted and distributed across the world [32]. This is beneficial to both manufacturers and end-users in terms of aspects like access to raw materials, cost efficiency, risk diversification, and environmental considerations. However, the nontransparent and complicated nature of such a supply chain model allows for stealthy intrusions that may compromise the authenticity of battery systems. In this section, we will first present the (Li-ion) battery supply chain model. Next, the vulnerabilities at each stage of the supply chain are discussed in detail.

A. Battery Supply Chain Overview

Fig. 2 illustrates a typical Li-ion battery supply chain where multiple actors collectively participate in transforming raw mineral materials into battery packs, production distribution, in-field usage, and battery end-of-life. The lifecycle of Li-ion batteries can be generally divided into the following stages, i.e., material phase, battery production phase, BMS development and integration phase, distribution phase, and in-field & end-of-life phase.

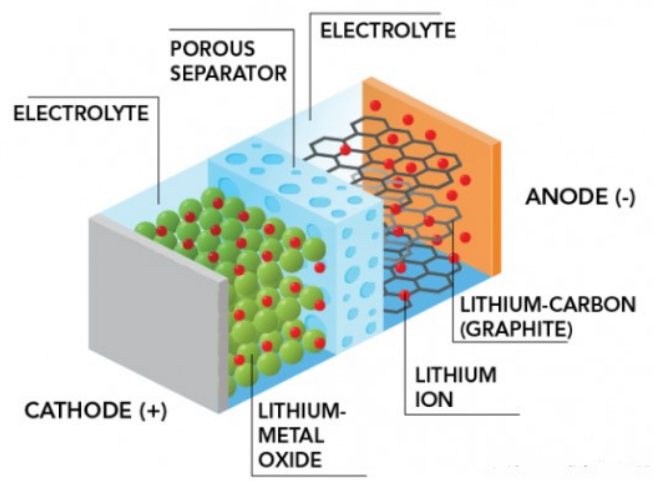


Fig. 3. High-level structure of a standard Li-ion battery cell [33].

1) Material Phase: As depicted in Fig. 2, raw material suppliers, or mining industries, are responsible for providing the downstream original battery manufacturer (OBM) with chemical sources [36]. Specifically, they first identify and explore available mineral reserves where sediments along with useful minerals can be extracted from. These ores are then transported to a facility such that they are processed to remove extraneous impurities, refined, and concentrated to a quality suitable for battery manufacturing. For example, principal materials in modern Li-ion batteries consist of lithium, cobalt, graphite, etc. As of 2023, Chile and Argentina export most lithium carbonate while Congo and China are the largest exporters of cobalt and graphite [37].

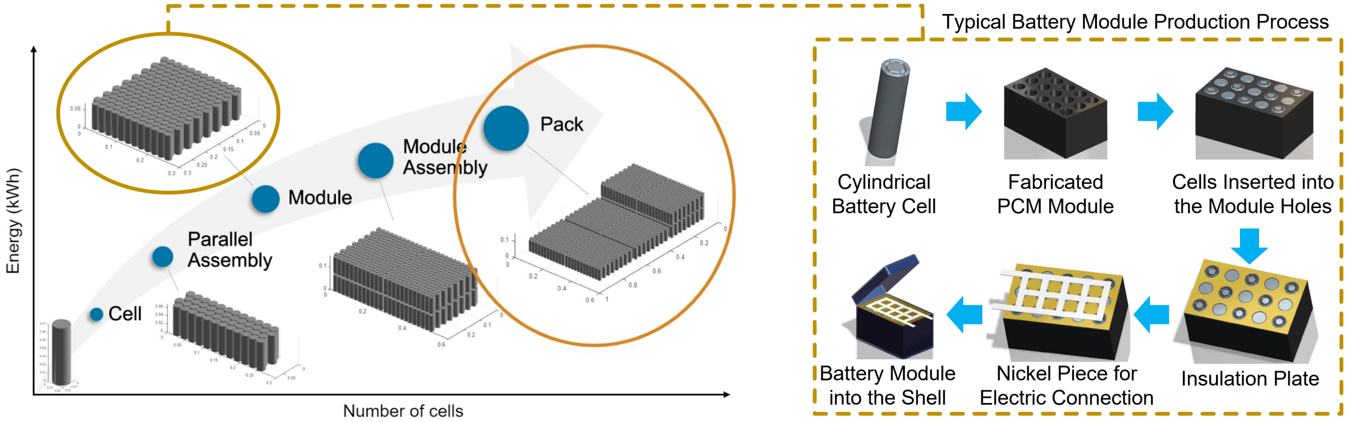

Typical Battery Module Production Process
Energy (kWh)
Number of cells
Cell
Parallel Assembly
Module
Module Assembly
Pack
Cylindrical Battery Cell
Fabricated PCM Module
Cells Inserted into the Module Holes
Insulation Plate
Nickel Piece for Electric Connection
Battery Module into the Shell

Fig. 4. Battery production phase [34]: The battery cell is fabricated using chemical sources from raw material suppliers. Multiple battery cells can be connected as a battery module by following the flow [35] as depicted on the right side. Battery modules can be further stacked and packaged in parallel to be a battery pack providing higher energy capacity and voltage levels.

2) Battery Production Phase: With the raw mineral materials from upstream suppliers, OBMs can produce battery packs by following the substages, i.e., battery cell production, battery module production, and battery pack assembly.

(i) Battery Cell Production: Li-ion battery cells can be produced using the materials from the suppliers [33]. Fig. 3 depicts a typical battery cell where it is made up of four main components, i.e., two electrodes (one anode and one cathode), a separator between two electrodes preventing unintended contact/shorting, and a liquid electrolyte medium enabling the movement of Li-ions between the electrodes [36]. Note that the anode and cathode are responsible for holding Li-ions when charged and discharged, respectively. The cathode can be a mixture of multiple metals (nickel, cobalt, lithium, others) while the anode is typically made of graphite such that electrolytes at different sides of the porous separator correspondingly contain lithium-metal oxide and lithium-carbon (graphite). When the battery is discharging, positive lithium ions (Li+) will be moved from the negative anode to the positive cathode through the electrolyte. An opposite behavior of these Li+ can be seen during the charging cycle [33].

(ii) Battery Module Production: A high-power application like EVs typically requires up to hundreds of volts for normal operations whereas a single Li-ion battery cell features only 3-4 volts. Therefore, battery cells need to be connected in series/parallel as serviceable units to provide desirable voltage and capacity. On the right side of Fig. 4, the flow of arranging battery cells into a module as an intermediate level of energy storage is depicted. Specifically, cylindrical battery cells from the previous phase are inserted into the holes of the pre-fabricated phase change material (PCM) case. Also, thermocouples, lightweight sensors measuring ambient temperatures, will be placed symmetrically into the PCM module as well for safety monitoring purposes. Battery cells are next insulated and connected using nickel pieces to become a functional module [35].

(iii) Battery Pack Assembly: As presented in Fig. 4, assembling battery modules into a cohesive battery pack involves a systematic and precise process to harness the combined power of individual cells. Initially, identical battery modules, each comprising multiple cells, are selected based on their voltage, capacity, and chemistry to ensure uniformity. These modules are then arranged and interconnected, typically using conductive materials and busbars, in a configuration that optimizes the overall voltage and capacity of the pack. Mechanical components, such as housing and thermal management systems, are integrated to ensure safety and efficient heat dissipation. Finally, the assembled battery pack undergoes rigorous testing by OBMs to validate its performance, safety features, and reliability under various conditions. The meticulous assembly of battery modules into a pack is crucial to meeting the specific requirements of the intended application.

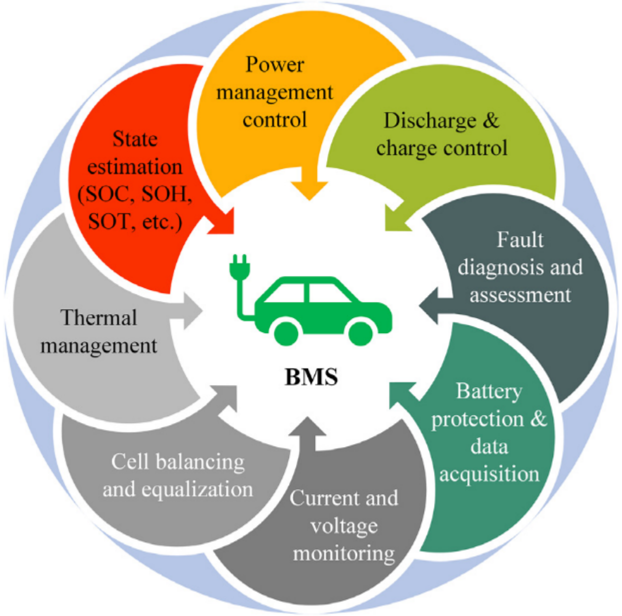

Power management control
Discharge & charge control
Fault diagnosis and assessment
Battery protection & data acquisition
Current and voltage monitoring
Cell balancing and equalization
Thermal management
State estimation (SOC, SOH, SOT, etc.)
BMS

Fig. 5. Functionality of a battery management system [38].

3) BMS Development and Integration Phase: Given their importance, fewer and fewer Li-ion batteries operate in a standalone manner, especially in prevailing applications such as

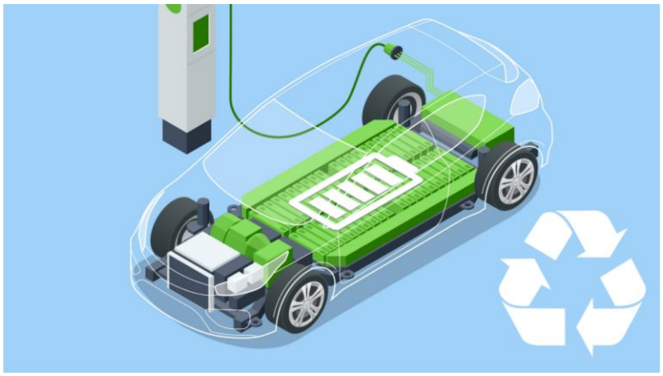


Fig. 6. Integrated batteries into electric vehicles [43].

portable electronic terminals and EVs. Instead, *smart battery packs* become the mainstream [39], i.e., a conventional battery pack is enhanced with a microelectronic BMS. A BMS can effectively enable a set of useful functionalities as depicted in Fig. 5, e.g., battery current/voltage monitoring, state estimation, and thermal management such that operating systems or users can easily visualize and control the battery status. More details regarding BMS and its assurance concerns can be found in Section III. As presented in Fig. 2, BMS developers are responsible for completing the system design involving software applications, microcontroller/microprocessor firmware, and printed circuit board (PCB) layout. In order to achieve shorter time-to-market and lower cost, BMS developers may tend to outsource the volume manufacturing to contractors, i.e., BMS manufacturers in Fig. 2, for PCB populations and device programming [40–42].

4) Distribution Phase: Once the battery pack is assembled and the BMS is integrated, the packs will enter distribution channels. In many cases, large original equipment manufacturers (OEMs) or product integrators like Tesla work with various suppliers to acquire their battery packs. These suppliers may be located globally, and there are agreements and contracts in place to ensure a steady and reliable supply chain. As for smaller companies or startups, they may tend to procure battery packs from distributors in the open market. Once the battery packs are manufactured and ready for distribution, they need to be transported to the assembly plants where equipment is being produced. This involves logistics planning to optimize transportation routes, modes of transport (such as trucks, ships, or planes), and scheduling to meet production demands. Note that, as depicted in Fig. 2, distribution channels entail not only battery packs but also microelectronic BMS which is necessary for smart batteries.

5) Product Integration Phase: The product integrator, e.g., EV integrator or smartphone integrator, would order smart battery packs from specified OBMs or distribution channels. For example, as depicted in Fig. 6, battery packs with integrated BMS are installed into the chassis of EVs in a way that ensures safety, stability, and efficient use of space [43]. The high-voltage component in the battery pack is then wired to the electric motors, inverters, and control systems. Rigorous quality control measures are also indispensable to guarantee that each battery pack meets safety and performance standards in the context of EVs. Finally, the BMS in the battery pack needs to be seamlessly interfaced with the EV software systems for effective usage and communication. Integrating Li-ion battery packs into other applications is supposed to follow a similar flow [43].

6) In-field and End-of-life Phase: During the in-field phase, the battery pack serves as the primary energy storage system for the application while the BMS continuously monitors and manages the pack's performance, ensuring optimal efficiency and safety. At the end of the battery pack's life cycle, recycling becomes a critical step. Recycling facilities are equipped to dismantle and recover valuable materials from the battery pack, including metals like lithium, cobalt, nickel, and other components. Proper disposal of batteries is crucial to prevent environmental contamination so recycling facilities are expected to adhere to regulations for the safe disposal of any non-recyclable or hazardous materials. Some batteries may not be suitable for their original application anymore because of reasons like reduced capacity or insufficient voltage whereas they can have a ”second life” by being repurposed for other applications of lower requirements. It is noteworthy that improper recycling or malicious counterfeiters are the primary source of battery authenticity concerns as discussed in Section II-B.

B. Supply Chain Vulnerabilities

Each stage of the Li-ion battery supply chain has been detailed in Section II-A. In addition, we also classified major entities in Fig. 2 into untrusted (in red) and trusted (in green) entities. Overall, most entities could be malicious indicating that the convoluted battery supply chain is confronted by a variety of vulnerabilities at each stage. In the following, we will discuss these vulnerabilities at each supply chain stage in terms of ❶ potential security problems, ❷ possible attack surfaces, and ❸ real-world attack examples.

1) Material Phase Threats: As the very beginning phase of the entire battery supply chain, malicious material suppliers may tend to provide impure or adulterated sources to reduce their costs. Such sources would affect the battery product quality and authenticity.

❶ ***Security Problems:*** Battery material replacement fraud refers to the illegal or unethical practices of swapping or modifying the battery materials of electric and electronic equipment without proper authorization or disclosure. This can harm the performance, safety, and environmental impact of any electrical equipment, as well as the consumers, manufacturers, and regulators. Adulterating or changing material composition produces weak or low-capacity batteries that may be hazardous or a loss of money for the consumers. Besides, inclement weather like hurricanes and tornadoes can disrupt infrastructures like shipping routes, pipelines, etc. impacting the timely delivery of raw materials. Geopolitical conflicts such as wars play a significant role in transporting battery materials within deadlines. Corporate consolidation is another important factor. The rapid technological invention is another blockage on the way to uniform distribution of battery materials [44].

❷ ***Attack Surface:*** There are several potential attack points in material level. Some corrupted persons may replace original materials with impure or low-quality ones [45]. Geopolitical conflict like any war may delay the timely delivery of battery materials [44]. Also, the monopoly of single companies [46] disrupts the uniform distribution of materials. If such a large company is affected by some catastrophe, the whole market space may be hampered.

❸ ***Real-world Examples:*** Lower-quality Li-ion battery products of bad materials will fail to meet the performance and safety standards. For example, such defective batteries will inherently generate much more heat than their counterparts manufactured with higher-purity materials, thus resulting in a shorter lifetime. A possible attack scenario of excessive heat is that the innermost plates in a prismatic battery (i.e., rectangular-shaped casing) have a difficult time dissipating the heat that is generated when the cell is operating under a heavy load as seen in [47].

2) OBM Phase Threats: OBMs gather material, electrolytes, and electrodes and follow some particular steps to produce batteries. It can be seen in Fig. 2 that we consider OBMs as the main trust anchor in the entire battery supply chain because they serve as the developers and stakeholders of the product battery pack. However, we still would like to discuss potential security issues at this stage briefly by taking *malicious insiders* into account.

❶ ***Security Problems:*** OBMs combine all the materials and electrodes to produce battery cells as explained in Section II-A2. Malicious insiders may mix impure materials with electrodes [48], adulterate the surroundings of the battery, and improperly label the casings at this level. Besides, as depicted in Fig. 3, principal components (electrolyte, electrodes, and separator) are brought together to one facility for cell preparation involving multiple steps, e.g. mixing, coating, compressing, slitting, drying, etc [49]. Adversarial insiders may introduce impurity at each step.

❷ ***Attack Surface:*** The electrolytes, electrodes, separators, and other ingredients are combined at the cell production level through some particular steps. In each of those stages, some adversaries may corrupt the materials and inject impure material there. Also, if the processes are not followed sequentially or there is a break of sequence, then a low-capacity battery may be produced. So every stage must be carefully monitored and taken care of to avoid any corruption.

❸ ***Real-world Examples:*** In 2017, a Japanese company (Mitsubishi Materials Co.) admitted that it had falsified data on the quality and performance of its aluminum products [50], which were used in the casings of EV batteries. The company had manipulated the inspection certificates to make the products appear to meet the specifications of the customers, affecting several major automakers.

3) Counterfeit Threats Involving Multiple Phases: Counterfeit battery is a very complicated supply chain management issue and fundamentally challenges battery authenticity. There is no single entity that has the resources and capabilities to accomplish such attacks but requires participation from many actors such as distributors, product integrators, and battery recyclers, instead as discussed below.

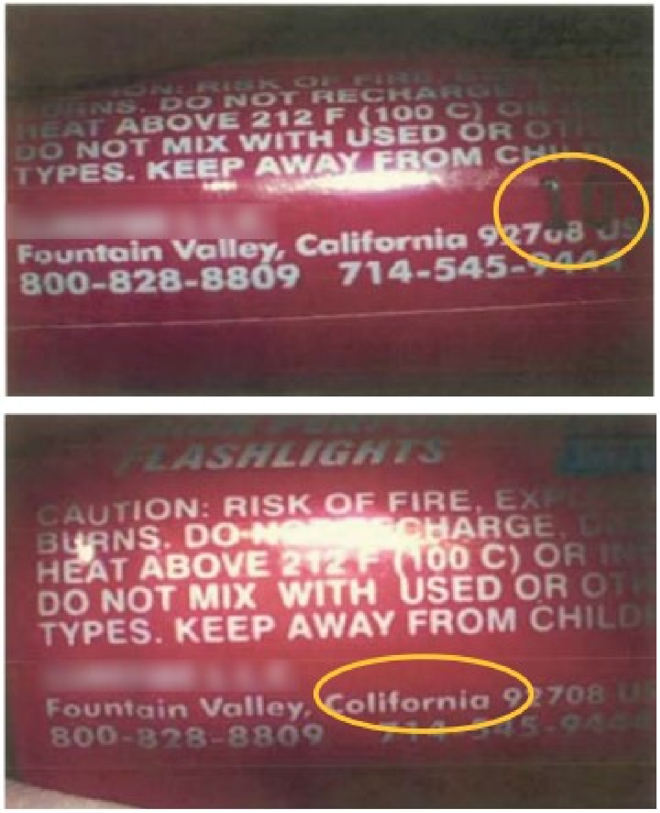


Fig. 7. An authentic battery (top) v.s. a counterfeit one (bottom). Counterfeit one has a misspelled 'California' and a missing stamp [51].

Module and package preparation of batteries are the most vulnerable and exposed parts of the supply chain that may be corrupted. Counterfeiting, rewrapping, and mislabeling are ever-prominent threats in battery module and package preparation [45].

❶ ***Security Problems:*** The counterfeit battery problem can be modeled into three major categories, i.e., recycled battery, rewrapped battery, and fake battery, as follows.

- **Recycled Battery:** In 1996, the United States Advanced Battery Consortium (USABC) first introduced a battery retirement criterion, i.e., a battery pack needs to be replaced when 20% of its original capacity is lost [52]. A retired battery pack needs to be recycled properly to minimize environmental hazards. However, untrusted battery recyclers may reclaim the end-of-life battery packs from some discarded systems/applications and rely on their collaborative distributors to sell them as new instances. For better marketing opportunities, such recycled battery packs typically carry a lower price tag compared to their genuine counterparts, thus attracting product integrators and entering user domain again.
- **Rewrapped Battery:** As the demand for good batteries is immense but supply is not abundant, some corrupt persons rewrap their fake batteries in the form of original ones and sell them to consumers [53]. These batteries have lower capacity and lower maximum discharge current than the original ones. Another kind of rewrapping happens at the distribution level, when module-level batteries reach for packaging, many corrupt individuals may separate the cells and repackage them displaying

incorrect capacity. This can jeopardize the credibility of the whole supply chain[53].

- **Fake Battery:** Fake batteries are unauthorized replicas or fakes of genuine products. However, they are still marketed to function with the tools, devices, or toys under a legitimate brand for unfair profits. Widespread demand for Li-ion batteries has facilitated illicit copying to profit through counterfeiting. Counterfeit cells are produced by copying high-quality products and deceiving unsuspecting customers. Fig. 7 shows a typical comparison between authentic and counterfeit fake batteries of the same model where one can clearly see there is a missing stamp on the package of the fake battery while the printing of *California* is misspelled as *Colifornia* as well. Note that, with the advancement of counterfeiting techniques, more and more fake batteries are deliberately labeled with the same trademark or logo as their genuine counterparts, making counterfeit detection based on merely visual inspection very challenging and even impossible.

❷ ***Attack Surface:*** As discussed, counterfeit batteries can be introduced at almost any stage of the supply chain. Low-quality and counterfeit battery packs may exhibit significant disparities between their advertised and actual achievable performance. Some manufacturers even promote performances that are unattainable for cells of that size and format. Customers often purchase these items unknowingly, as they seem superior to other similar cells. Identifying such discrepancies can be challenging, given the high variability in geometries and the diverse cathode and anode chemistry used in lithium-ion cells [54]. Additionally, application-specific designs may result in performance variations among seemingly identical cells. Therefore, it is essential to grasp the application-based requirements before purchasing or using any type of Li-ion cells.

❸ ***Real-world Examples:*** There are lots of real-world incidents of counterfeit batteries as summarized in Table I and II. We covered some of them in Section I already and would like to highlight three other cases below.

- **Fake Sony VTC5 Batteries:** These are supposed to be high-drain batteries with a capacity of 2600mAh and a maximum continuous discharge current of 20A. However, some counterfeit versions have been found to have a capacity of only 1600mAh and a discharge current of 10A or less [51].
- **Counterfeit Batteries in Hoverboards:** As of July 2016, the U.S. Consumer Product Safety Commission reported over 60 incidents in the United States where Li-ion batteries in hoverboards caught fire. These incidents resulted in the destruction of bedrooms and even entire homes, causing property damage exceeding USD 2 million[55]. More recent incidents can be seen in Table II.
- **Fake Samsung 25R Batteries:** These are popular batteries for vaping devices, with a capacity of 2500mAh and a maximum continuous discharge current of 20A. However, some counterfeit versions have been found to have a capacity of only 1200mAh and a discharge current of 5A or less. [51].

TABLE II
REPORTED FAKE BATTERY INCIDENTS [55].

Affected Sellers	No. of Reports	Last Updated
Amazon	855	Oct. 28, 2023
Walmart	133	November 20, 2022
eBay	127	March 13, 2021
Newegg	14	May 20, 2021
Wish	14	February 2, 2021
Internet vendors	8	March 21, 2020
Twitter	3	August 3, 2019

The impacts of counterfeit batteries can be significant. Counterfeit products pose numerous safety risks, as they are prone to failure and can cause fires and explosions. These illegal enterprises are typically run by manufacturers who lack the technical knowledge and understanding necessary for safety, quality control, and proper shipping practices. Certifications are often falsified, and misleading performance claims are made on the labels[51]. This leads directly to compromised safety of lithium-ion products and, ultimately, the devices that utilize them. In summary, counterfeit products demonstrate a lack of performance, quality, and safety compared to their genuine counterparts. Fake batteries can pose significant hazards, often lacking essential protective mechanisms. As a result, they are prone to overheating, explosions, and fire hazards, potentially causing severe damage to electronic devices or, in extreme cases, personal injuries. About 30 percent of the global battery market consists of counterfeit products [56]. In 2020, counterfeit batteries caused an estimated USD 20 billion in losses worldwide [56].

4) Consumer Phase Threats: When generalized consumers receive a product from a store, it is very unlikely that they can immediately know the internal situation of a product. Some adversaries may take advantage of this and put counterfeit batteries in the name of the original ones. Various aspects of this attack are described below.

❶ ***Security Problems:*** At the consumer level, general people do not have established equipment to examine batteries, making them prone to be easily deceived. Some adversaries take advantage of this and sell fake batteries in the name of the original ones. In recent times, online markets like Amazon and eBay have reported several instances of fake batteries in their store. Also, various consumers have reported their battery capacity to be lower.

❷ ***Attack Surface:*** Fire safety issues at the consumer level have been long discussed as a potential bottleneck in electrical and electronic equipment maintenance. Counterfeit or fake batteries may create additional risk as they give leverage to batteries having lower capacity.

❸ ***Real-world Examples:*** In a 2015 lawsuit, a woman injured by an exploded battery in an e-cigarette was awarded nearly USD 1.9 million from the local e-cigarette store, the distributor, and the wholesaler [57].

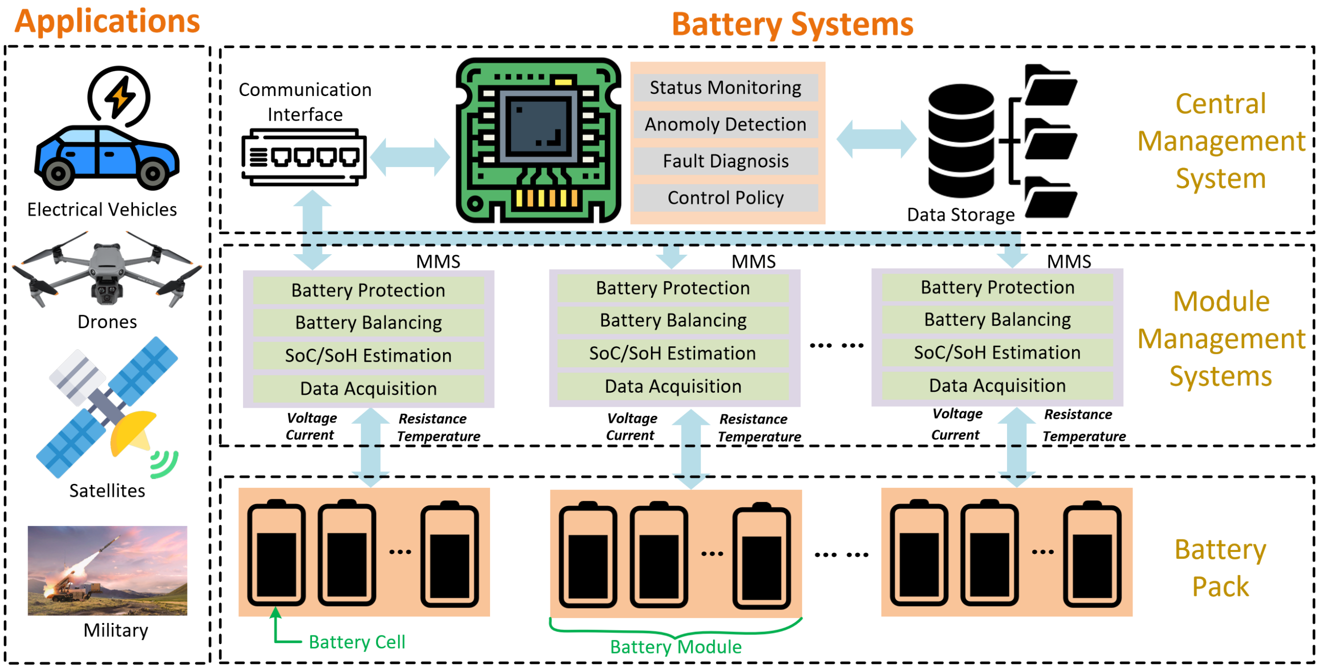


Fig. 8. Overview of a general smart battery system.

III. Battery Cyber-Physical Security Issues

In this section, we first present the overview of battery systems. Next, we cover the threat models regarding the assumptions and motivations of adversaries that challenge battery system assurance. Finally, we present our summary and perspectives on advanced attack vectors.

A. Overview

Battery systems are ubiquitous in numerous applications ranging from smart terminals to mission-critical infrastructure by manifesting as versatile variants with different sets of features depending on the particular products. On the other hand, as mentioned in Section II-A3, higher and higher requirements of safety and run-time monitoring inspire *smart battery systems*, i.e., conventional battery packs enhanced by BMS as presented in Fig. 8. A smart battery system typically consists of three main blocks. i.e., battery pack, module management systems, and the central management system.

1) Battery Pack: Li-ion battery packs power the applications. Depending on the specific applications, the parameters such as size, voltage, and capacity of the battery pack are different; for example, energy-intensive instances such as EVs and drones focus more on the power density and lifetime of the underlying battery pack whereas smaller devices like smartphones prefer lightweight batteries with a high energy density, i.e., they can store a large amount of energy in a relatively compact package. As detailed in Section II-A2, the basic building block of the battery pack refers to a *battery cell* that transforms chemical energy into electrical power. Multiple battery cells are then mechanically connected in series or parallel to be *battery module* as serviceable units. Further, a *battery pack* is comprised of battery modules and optional peripheral components like cooling/heating systems to deliver power to applications.

2) Module Management System: As mentioned, the battery pack status needs continuous monitoring and necessary corrections during run-time for system safety. Therefore, sensors and microelectronic-based control units are typically deployed for local battery management, which is collectively called module management systems (MMS) as illustrated in Fig. 8. There can be multiple MMS instances to enable fine-grained management of each battery module in the pack in the subsequent aspects.

- *Data Acquisition.* One of the most important tasks for each MMS is that it needs to closely quantify and collect status statistics of the target battery module and every internal battery cell. For example, the sensors sampled the voltage, current, temperature, and battery resistance and transferred them to the MMS for further analysis.
- *SoC/SoH Estimation.* To estimate the state-of-charge (SoC), i.e., the percentage of the remaining energy over the total battery capacity, MMS mostly utilizes the *Columb Counting* algorithm where the discharging current is measured and integrated over time. Also, the state-of-health (SoH) parameter, which represents the remaining capability and level of degradation of an in-use battery, can be estimated using the collected battery resistance.
- *Battery Balancing.* Additionally, the collected statistics can help guide *battery balancing* which can effectively extend the lifetime of the entire pack (battery cells connected in series). In detail, individual cells in a pack inevitably have inherent variations and different aging patterns. Cells with lower capacity feature a shorter charging/discharging cycle compared to others and thus

suffer from a higher risk of being overcharged/over-discharged. By balancing each cell to an equivalent SoC, the overall capacity can be maximized.

- Battery Protection. Battery safety can be the highest priority when it comes to the mission-critical infrastructure. Based on the analysis of the battery status, MMS can identify anomalous scenarios such as over-voltage and over-temperature that may result in pack leaking or even explosion. In response, MMS typically cuts off the MOSFET switch to dispatch the battery from the payload, avoiding further aftermaths.

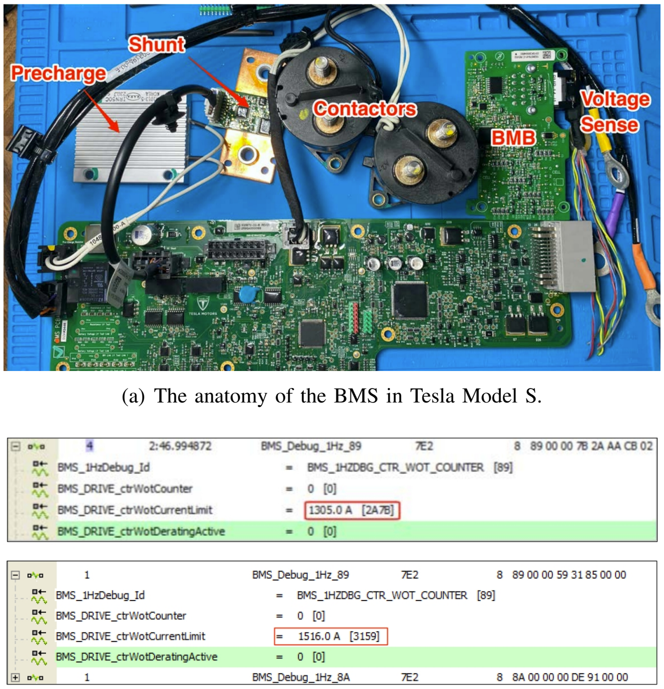
3) Central Management System: In addition to the capabilities provisioned by local MMS, there could be more sophisticated algorithms required for advanced battery management. Therefore, MMS is typically connected to the central management system (CMU) to jointly establish the *battery management system*. The connectivity could be a serial interface or a wireless channel depending on the physical layer of the master system. For example, serial interfaces such as I2C and SPI may be used when the CMU is implemented on a local microprocessor or other devices like FPGAs [17] on the same board of MMS for high cost-effectiveness. However, a practical challenge faced by the local CMUs is their insufficient processing capabilities. The performance of a commodity microprocessor can only be GBs per second at the fastest while the storage and scalability are limited as well given the large number (sometimes up to thousands) of battery cells in advanced applications like EVs or stationary charging facilities [58]. Moreover, state-of-the-art data-driven battery management algorithms, such as machine learning (ML)-based solutions, require massive historical data of battery behaviors for accurate analysis, further stressing the need for computational power and allocated memories [23]. To address such challenges, an increasing number of investments shift battery system architecture from local devices to cloud BMS [59] where a digital twin-based virtual central BMS is established on high-performance cloud servers [60]. As such, local module management systems can still be implemented on lightweight Internet-of-Things (IoT) devices for edge processing while the battery data can be transmitted to the cloud platform through wireless protocols. Heavy tasks such as data storage, statistics processing, and ML model deployment can be offloaded to the CMU on the cloud for improved efficiency and adaptability [60]. As a hybrid CPS, battery systems suffer from relevant security threats and concerns as detailed in Section III-B.

B. Cyber-Physical Assurance Concerns

As a cyber-physical device, battery systems should always preserve confidentiality, integrity, and availability to fulfill the assurance requirements. Violations of any security property would result in a variety of security compromises. For example, a compromised battery system may be degraded on purpose such that it cannot provide enough power for the electric vehicle on the highway or has a shorter lifetime because of accelerated aging. Even worse, catastrophic incidents might be induced by deliberate attacks resulting in life-threatening fire and explosion of the battery pack. Note that even the same aftermath could stem from different underlying attack vectors and thus call for systematic analysis and discussions. We will focus on the confidentiality, integrity, and availability issues around battery systems by ❶ presenting the potential security problems, ❷ analyzing the attack surface comprehensively given state-of-the-art security techniques, and ❸ illustrating real-world attack examples.

TABLE III
CONFIDENTIALITY CONCERNS ON BATTERY MANAGEMENT SYSTEMS.

Confidentiality Concerns	Attack Effects	Severity
Sensitive Data Access	Insights into the overall system.	★
Unauthorized Credentials Access	Unauthorized access to the system.	★ ★ ★
Intellectual Property Theft	Competitive advantage in business.	★ ★
Privacy Concerns	Compromising user privacy.	★ ★ ★



(a) The anatomy of the BMS in Tesla Model S.

```
⊟  4     2:46.994872     BMS_Debug_1Hz_89     7E2     8  89 00 00 7B 2A AA CB 02
   BMS_1HzDebug_Id                    =  BMS_1HZDBG_CTR_WOT_COUNTER  [89]
   BMS_DRIVE_ctrWotCounter            =  0  [0]
   BMS_DRIVE_ctrWotCurrentLimit       =  1305.0 A  [2A7B]
   BMS_DRIVE_ctrWotDeratingActive     =  0  [0]
```

```
⊟  1                     BMS_Debug_1Hz_89     7E2     8  89 00 00 59 31 85 00 00
   BMS_1HzDebug_Id                    =  BMS_1HZDBG_CTR_WOT_COUNTER  [89]
   BMS_DRIVE_ctrWotCounter            =  0  [0]
   BMS_DRIVE_ctrWotCurrentLimit       =  1516.0 A  [3159]
   BMS_DRIVE_ctrWotDeratingActive     =  0  [0]
⊞  1                     BMS_Debug_1Hz_8A     7E2     8  8A 00 00 00 DE 91 00 00
```

(b) The parameters of available power (in Amps). The top refers to the power available before firmware tampering 1305.0A while the bottom gets 1516.0A.

Fig. 9. Reverse engineering the BMS of Tesla Model S and firmware tampering to increase the available power [19].

1) Confidentiality Concerns: Battery systems measure and store precise battery statistics which can be valuable for adversaries. Moreover, the battery management system design involves lots of R&D efforts, making itself intellectual properties which may become the targets of attackers. Therefore, intrusions on battery management systems can effectively induce confidentiality concerns.

❶ ***Security Problems****:* We summarize and tabulate the major confidentiality concerns in Table III along with corresponding attack effects and severity. Specifically, confidentiality concerns involve (i) *sensitive data access*, (ii) *unauthorized credentials access*, (iii) *intellectual property theft*, and (iv) *privacy concerns* as presented below.

(i) *Sensitive Data Access:* As discussed in Section III-A, battery systems are responsible for storing and processing sensitive information of battery status including but not limited to SoC, voltage, temperature, and health (e.g., resistance). Once the confidentiality of such sensitive information is violated, adversaries will obtain unauthorized insights into the overall system, usage patterns, and potentially the activities. We identify the concern itself at relatively low risk in Table III since sophisticated analysis and efforts are still needed to intelligently exploit the information. However, for capable adversaries, the leaked information can be very helpful in deducing more valuable in-system assets of battery-operated devices or assist in compromising the targets further.

(ii) *Unauthorized Credentials Access:* In most applications like smartphones and EVs, battery systems need to communicate with other components frequently to report the status of physical battery packs or enforce high-level battery management policies. Therefore, battery systems often store security credentials or secret keys to protect in-system communication. If adversaries can successfully attack the system to expose these assets, they might manage to intercept the communication for further analysis. Given that leveraging security credentials to compromise system security is pretty intuitive, we think this is one of the biggest concerns as illustrated in Table III

(iii) *Intellectual Property Theft:* As one can see in Fig. 8, BMS is a complicated system involving monitoring, control theories, (wireless) communication, and even cloud/database techniques. Experienced adversaries, especially engineers from competitor companies, may attempt to break down the system, understand the architecture, and figure out the core techniques incorporated in the BMS product. As such, the competitive advantages of BMS original designers would diminish because of intellectual property theft. Although the infringement is sometimes forbidden legally, it is costly to thwart or adduce evidence for startups and individual developers.

(iv) *Privacy Concerns:* The statistics collected and stored by battery systems could characterize the user identity, thereby raising privacy concerns. For example, adversaries with unauthorized access to battery status can utilize battery capacity, SoC, SoH, etc. to construct a user identity and track the user activities (we present a real-world example *the leaking battery* is presented in ❸ ***Real-world Examples*** to support this argument). Besides, EVs always track the location and usage patterns of the vehicle; user privacy would be completely sacrificed once the data is intercepted by attackers when interacting with battery systems.

❷ ***Cyber-Physical Attack Surface Analysis****:* As discussed, battery systems hold security assets such as SoC, SoH, and temperature which can be exploited by adversaries to compromise the application security.

(i) *Snooping Attacks:* In snooping attacks, adversaries tend to eavesdrop on the data communication either on the in-system bus, e.g., CAN/SPI bus, or the wireless connectivity. If strong encryption is not in place, the confidentiality of exploitable information could be violated. [58] discusses an attack scenario where attackers can procure the bandwidth information between MMS and CMS through snooping attacks. The bandwidth information can be further analyzed to figure out which components/features of BMS are active and what kind of activities are currently performing.

(ii) *Man-in-the-Middle (MitM) Attacks:* MitM is a prevalent cyber attack vector where a third-party adversary can position herself between the client and server during the conversation [61] to either eavesdrop or even impersonate one of the entities. In battery systems, MitM attacks are possible threats especially when the CMU is a cloud-based platform [60], i.e., the link between module management systems and CMUs refers to network communication in Fig. 8. Moreover, MitM attackers may intercept communication between components within the BMS or between the BMS and external systems. This can lead to the unauthorized access of sensitive data transmitted over communication channels, resulting in confidentiality concerns.

(iii) *CMS Database Intrusions:* The CMS tasks like ML algorithms sometimes require a large amount of history data, making the database a promising target of adversaries. Concerning confidentiality attacks on the cloud database, a very popular attack vector is SQL injection [62] where network hackers utilize malicious SQL code to intrude the backend database especially when its access control policies are not well-designed. Through web page input or open API, SQL injection can enforce the replacement of malicious code in SQL statements, gaining access to sensitive data for further exploitation.

(iv) *Brute-force Attacks:* Attackers or malware may attempt to log in to the BMS or applications by systematically trying different combinations of usernames and passwords until the correct credentials are found. If weak authentication mechanisms or default credentials are used, unauthorized access will be granted and consequently compromise confidentiality. Although this sounds a bit naive and far-fetched, it surprisingly results in significant real-life impacts. A famous example is Mirai Botnet [63] which is a malware infecting numerous smart devices in 2016 and remotely controlling them as *zombies*. The root cause of the success of Mirai botnets (i.e., a massive and global denial-of-service attack) came down to a very simple fact; users of IoT devices barely have the security awareness and thus adopt the default username-and-password combo such that Mirai Botnet can easily hijack the systems.

(v) *Reverse Engineering:* BMS is a hybrid system involving software, firmware, and hardware [17] exposing an extensive attack surface of reverse engineering and resulting in subsequent IP piracy infringement of BMS developers. Software reverse engineering could retrieve the high-level functionality of BMS, e.g., the software algorithms executed on a microprocessor-based MMS, from low-level binaries. There have been mature disassmblers and utilities developed for software reverse engineering such as IDA Pro [64] and Ghidra [65]. Firmware reverse engineering can rely on similar tool chains to its software counterparts if platforms are supported. Although quite a few microprocessor/microcontroller platforms have been covered by state-of-the-art tools, there are some FPGA-based MMS that remain unsupported because of totally different working principles of underlying devices. Unlike sequential executions of instructions on microprocessors, FPGAs are inherently parallel circuitry programmed with binary configuration files, so-called bitstream [66]. On the other hand, mainstream FPGA manufacturers are reluctant to reveal the vendor-specific bitstream format for their *security-by-obscurity* strategies [67]. Unfortunately, such strategies have been demonstrated to be in vain given the fact that bitstream reverse engineering techniques [66–69] can crack the bitstream format accurately by only exploiting the official EDA tools like AMD-Xilinx ISE or Vivado. As for hardware reverse engineering, it has been widely recognized as a challenging task [70] where adversaries need to reconstruct the physical design of integrated circuits (ICs) from the post-silicon devices involving decapping, chemical processing, layer-by-layer imaging, and sophisticated analysis & reconstruction [71]. In the context of BMS reverse engineering, we think IC reverse engineering may be unlikely for adversaries because they have the chance to identify the chip model and specification from the marking on the chip surface and simply purchase the same ones from the open market. Therefore, software and firmware reverse engineering call for more awareness and investment in IP protection from the perspectives of BMS developers.

(vi) *Malicious Insiders or Social Engineering:* Individuals with authorized access to the BMS, such as employees or contractors, may intentionally or unintentionally compromise confidentiality. This can occur through actions like data theft, sabotage, or unauthorized data access. Besides, attackers may use phishing emails or other social engineering techniques to trick individuals with access to the BMS into revealing sensitive information, such as login credentials.

(vii) *Physical Side-channel Attacks:* As the local battery system is implemented on hardware devices, adversaries could observe their run-time physical properties such as power consumption and electromagnetic (EM) emissions to deduce confidential information, i.e., so-called side-channel attacks [72]. The security credentials like session keys may be deduced from the switching activities of underlying circuitry, leading to further confidentiality compromise. In addition to breaking cryptographic algorithms on hardware, side-channel attacks can assist adversaries in understanding BMS functionality and timing to enable more sophisticated attacks. Note that physical access or proximity is prioritized by adversaries but remote compromise remains possible especially when multiple control blocks share the same FPGA fabric. As discussed in [73], a typical scenario refers to a main controller consisting of two control modules on the same FPGA. There is a proper isolation fence (i.e., blank configurable resources [74]) between the two logic circuitry to avoid logical interference. However, if one of the control logic is accessible to cyber-attackers, they can still enable power side-channel attacks by implementing a lightweight power sensor to acquire switching activity profiles from the other (victim) portion [75].

❸ ***Real-world Examples**: The leaking battery* [76] research reveals real-world confidentiality concerns regarding battery management systems, i.e., *sensitive data access* in the BMS has been effectively exploited to raise *privacy concerns*. Specifically, some HTML5 browsers provide the website side with an application programming interface (API) to access the battery status. Using this API, websites can easily access the battery information such as capacity and SoC without any permissions or awareness from users. The data collection was originally intended to help balance the performance and energy cost, e.g., the website can switch between high-performance or energy-saving modes given the SoC of your laptop/smartphone. However, the high-precision battery information simultaneously enables fingerprinting and tracking user online activities in short time windows. The experiments in [76] demonstrate the effectiveness of the exploits by reconstructing user identifiers on Linux Firefox browsers. Most mainstream browsers were affected except for the Tor Browser which completely disabled the battery status API. To mitigate the threats, the authors also suggest limiting the precision of battery SoC readouts and/or improving the API sensitivity by asking for user permissions before activation.

TABLE IV
INTEGRITY CONCERNS ON BATTERY MANAGEMENT SYSTEMS.

Integrity Concerns	**Attack Effects**	**Severity**
Data Manipulation	Deceiving the system into wrong decisions and unsafe conditions.	★★★
Safety System Bypass	Put the physical battery at risk of damage or failure.	★★★
Falsification of Battery Health	Premature battery replacement or allowing for recycled batteries.	★★
Hardware Tampering	Tampering with HW components, e.g., sensors, to affect the system.	★★

In BlackHat 2020, [19] presents an attempt to reverse engineer the BMS of the Tesla Model S electrical vehicle. The researcher breaks down the car model and reverse engineer the system as illustrated in Fig. 9(a). The main microprocessor (i.e., the CMS in Fig. 8) is TI TMS320C2809 while an Intel (formerly Altera) CPLD serves as the hardware backup. One can see the current shunt (battery current measurements), precharge resistor (damage prevention), battery balancing components (i.e., BMB), etc. in Fig. 9(a) as well. Besides hardware reverse engineering, [19] also cracks the firmware for BMS using IDA Pro to retrieve the source code, which might result in *intellectual property theft*.

2) Integrity Concerns: As discussed in Section III-A, BMS plays a pivotal role in ensuring the performance, security, and safety of the battery pack. Therefore, the integrity of battery systems becomes essential to ensure their compliant behaviors and effective management; we present the potential concerns, attack effects, and severity in Table IV.

❶ ***Security Problems**:* Table IV covers four major integrity concerns of battery systems, i.e., (i) *data manipulation*, (ii) *safety system bypass*, (iii) *falsification of battery health*, and (iv) *hardware tampering*.

(i) *Data Manipulation:* Maliciously manipulating the critical data in battery systems can result in catastrophic aftermaths. For example, altering the SoC data of the specified battery from high to low can deceive the control system into the wrong decision of continuing the charging state beyond its capacity. The consequent overcharging can be extremely risky in inducing thermal runaway, reducing battery lifetime, and causing fire/explosion hazards. Similarly, other anomalous scenarios such as undercharging, over-temperature, and under-temperature can be triggered in a similar fashion.

(ii) *Safety System Bypass:* Battery systems often include safety features and protections to prevent hazardous conditions such as overheating or overcharging. An attacker might attempt to bypass or disable these safety mechanisms, by altering critical data as discussed or even tampering with the hardware, putting the battery and the overall system at risk of damage or failure.

(iii) *Falsification of Battery Health:* Altering the reported health status (e.g., the internal resistance of battery cells) of the battery can mislead users and system operators. This could lead to premature replacement of batteries that are still serviceable or, conversely, the use of batteries that pose a safety risk.

(iv) *Hardware Tampering:* Besides high-level software algorithms in module management systems and central management systems, hardware infrastructure like wiring, sensors, and transistor switches is also indispensable to maintain functionality and guarantee safety. Tampering with hardware can result in wrong readings, ineffective circuit breaker protection, and failure in transmitting sensitive signals (e.g., warning or reset signals).

❷ ***Cyber-Physical Attack Surface Analysis****:* The integrity of BMS is a critical aspect for ensuring the overall assurance as arbitrary falsification of sensitive data might lead to misjudgment and wrong decisions at higher levels, further inducing serious aftermath.

(i) *False Data Injection:* Attackers can deliberately manipulate the packets from MMS to CMS. The manipulation can entail original data like measurements of voltage, current, and temperature or direct commands. The former could disrupt or mislead the algorithms running on the CMS for, e.g., false SoC/SoH estimation while the latter can even gain access to the entire battery pack [58]. Falsified SoH data may trigger premature battery replacement or allow for recycled batteries as seen in Table IV. Similarly, false estimation of SoC can also significantly jeopardize normal operations of EVs, e.g., low maneuverability of EVs or misinforming drivers about the achievable performance [58].

(ii) *Random Delay Attacks:* A random delay can be deliberately introduced to the sequence of BMS commands or data [58]. For example, when BMS detects undesired anomalies and would like to cut the battery power from the application, the security commands may be delayed intentionally to prevent successful protection.

(iii) *Replay Attacks:* A replay attack is a type of cyber/bus attack where an attacker intercepts and maliciously retransmits data that was previously recorded. As such, even if the traffic is encrypted, the attacker does not need to decrypt the data; instead, they simply capture the data packets and replay them to the target system or network. If timestamps or unique session identifiers are not included in BMS communication, adversaries may gain access to the entire system by replaying the recorded credentials [58].

(iv) *Communication Protocol Integrity Attacks:* The CAN bus is one of the most prevalent protocols for in-system communication of battery systems because of its cost-effectiveness and robustness. However, the CAN bus does not have enough authentication capabilities and thus enables a variety of integrity attacks [73]. As for wireless communication, the MQTT protocol is typically used for battery systems. The topology of MQTT is that a publisher can broadcast messages of a topic to subscribers who request the same topic through a broker. However, it has been found that malicious subscribers can also control the broker since the broker listens to all messages sent to it including false ones [77],

(v) *Malicious Firmware Updates or Tampering:* Attackers may compromise the integrity of BMS firmware, leading to altered functionality, unauthorized access, or incorrect processing of critical functions. The compromise can be implemented through either malicious firmware updates or local tampering. Malicious firmware updates can be achieved by direct falsification of the packets if strong authentication is not in place. Sometimes adversaries may tend to roll back the firmware version to previous ones through replay attacks. Such attacks can not only defeat encryption protection but also disable added security features [78]. As for local tampering, attackers with physical access to on-chip firmware storage may read the firmware, apply modifications, and reload it. Note that some devices like mid/high-end FPGAs feature hardware cryptographic engines to thwart straightforward integrity attacks. However, sophisticated attackers developed intelligent strategies to break the protection as well [79, 80].

(vi) *Physical Fault Injection:* Physical fault injection refers to the attacks where adversaries intentionally change inputs or physical parameters/environments of the underlying MMS hardware to interrupt its normal operations. The common methods involve premature clocks, voltage drops, EM disturbances, and laser pulse [81]. As discussed in [82], the negative impacts of fault injection can bypass built-in security mechanisms, assist in advanced fault analysis of ciphers, escalate the user privileges, etc.

(vii) *Hardware Trojan Insertion:* Hardware Trojan is a long-standing concern in the hardware security domain [83–85] which essentially refers to the malicious circuitry that gets into the IC at different stages including design, integration, and manufacturing [85]. If the BMS is built on top of untrusted hardware ICs, adversaries could be very potent to falsify the sensitive data covering the measurements and credentials. Also, hardware Trojan attack models can be versatile, and successful Trojan insertion implies the dominance of the entire system against any countermeasures or mitigation at firmware and software levels because the security measures can be fundamentally disabled at the hardware [27, 86–89].

(viii) *Interference from Other In-system Components:* In complicated applications such as EVs, other in-system components/devices may talk to the local BMS (i.e., MMS) or maliciously affect the compliance of MMS. As discussed in [73], the widely used CAN bus protocol possibly allows for masquerade attacks [90] and replay attacks [91] such that adversaries who gain access to either one of the on-board controllers or the CAN-USB interface could broadcast fake messages to battery systems and/or main controllers. For instance, the malicious components can pretend to be MMS sending packets including erroneous data like SoC, voltage, and temperature, resulting in subsequent damage because of over-charging or overvoltage.

❸ ***Real-world Examples****: Battery firmware hacking* [92] presents an in-depth analysis of the entire smart Li-ion battery pack in quite a few Apple products including MacBook,

TABLE V
AVAILABILITY CONCERNS ON BATTERY MANAGEMENT SYSTEMS.

Availability Concerns	**Attack Effects**	**Severity**
Denial of Service (DoS)	Leading to the downtime of the system.	★★★
Accelerated Battery Aging	Reduced battery lifetime and unnecessary financial lost.	★★
Battery Health Monitoring Disruption	Premature battery replacement or allowing for recycled batteries.	★★
Battery Draining Attacks	Aggressively consume the energy to end the system lifetime earlier.	★★★

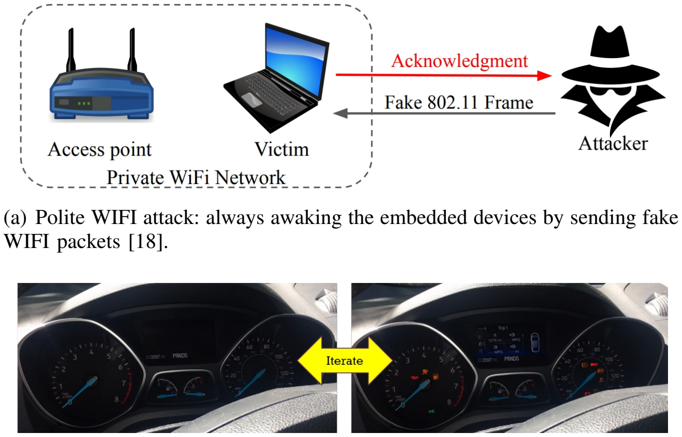
MacBook Pro, and MacBook Air laptops. The researchers first reverse-engineer the firmware content and firmware flashing procedure of the embedded battery controller, i.e., they can reconfigure the smart battery by modifying the firmware (i.e., *data manipulation*). This is allowed because Apple unintentionally adopts the same credentials for unsealing the battery and granting full access to the pack so the researchers can repurpose the information. Besides, the checksum of ensuring firmware authenticity can be bypassed (i.e., *safety system bypass*) to allow for the execution of tampered firmware. By tampering with the firmware, the adversary offers a simple API that can read and make arbitrary changes to parameters and data. Such overall control and subsequent modification are enough to result in serious safety concerns, e.g., changing the SoC can easily deceive the battery into over-charging or even fire.

Tesla BMS cracking [19] can not only raise confidentiality concerns as discussed in Section III-B1 but also have the implications of integrity violations. Based on the knowledge from hardware and firmware reverse engineering, the adversary can effectively modify the system to unlock the unavailable power/features given the specified version. For example, Tesla restricts the maximum speed/acceleration of their vehicles by controlling the peak power from the battery pack. In [19], the limitations of available power can be unlocked as depicted in Fig. 9(b); the maximum available current is 1305.0A before whereas firmware tampering can increase it to 1516.0A. Note that, in addition to firmware tampering, the shunt hardware in Fig. 9(a) needs to be modified (i.e., *hardware tampering*). A single wire is connected from the shunt to the CPLD which would help BMS generate an alert after firmware tampering preventing the contactors from being closed. Therefore, a breakout board is necessary to monitor the signal before driving the car.

3) Availability Concerns: As the power source, compromising the battery availability can fundamentally brick the entire system. We highlight four availability concerns in Table VII.

❶ ***Security Problems****:* Table VII presents (i) *denial of service (DoS)*, (ii) *accelerated battery aging*, (iii) *battery health monitoring disruption*, and (iv) *battery-draining attacks*. Although some of the concerns seem to be similar to integrity ones such as battery health monitoring disruption, the goal of availability compromise refers to simply disabling the feature by any means instead of deliberately modifying it, which is more straightforward and less demanding of attack setup/expertise.

(i) *Denial of Service:* Attackers may launch denial-of-service attacks on the BMS, overwhelming it with a high volume of requests or malicious traffic. This can lead to the BMS becoming unresponsive, causing downtime and preventing the system from functioning as intended.



(a) Polite WIFI attack: always awaking the embedded devices by sending fake WIFI packets [18].

(b) Adversaries can inject messages into the CAN bus of the vehicle to prevent the system from felling asleep [93].

Fig. 10. Real-world battery draining attacks on battery-powered embedded devices and EVs.

(ii) *Accelerated Battery Aging:* Attackers may compromise BMS to disrupt the overcharging/discharging protection or battery balancing functionality so that batteries can be significantly degraded and damaged. As such, battery aging is accelerated; the victim battery pack will not be able to meet the lifetime promise and lead to unnecessary financial and economic loss.

(iii) *Battery Health Monitoring Disruption:* A BMS is responsible for monitoring the health of the battery and implementing safety measures when necessary. An attack that disrupts the monitoring functions can lead to a lack of awareness regarding the state of the battery, potentially resulting in unsafe operating conditions.

(iv) *Battery-draining Attacks:* Most battery-operated embedded devices and EVs support advanced features such as low-power modes and run-time power-saving measures to extend the battery life. However, adversaries may exploit vulnerabilities in the system/application to intentionally increase its power consumption, leading to accelerated battery depletion. For instance, attackers may either force the device to continuously perform resource-intensive operations or send fake requests to the target devices to prevent them from staying in low-power mode. The consequence of battery draining can be severe resulting in service outages, data loss, and even safety risks.

❷ ***Cyber-Physical Attack Surface Analysis****:* The availability of a battery system is crucial to assurance because it directly impacts the reliability, performance, and safety of battery-powered systems.

(i) *Network Flooding Attacks:* Network flooding attacks can severely impact the availability of battery systems by overwhelming its network infrastructure with a deluge of traffic. In such an attack, malicious actors exploit vulnerabilities in the system to flood the IoT-based MMS with an excessive volume of data packets or requests, rendering them unable to respond to legitimate traffic effectively [94]. This flood of network traffic exhausts the system's resources, including processing power, memory, and bandwidth, leading to degraded performance or complete system failure. In the context of a battery system, which is critical for monitoring and controlling battery health and performance, such attacks can disrupt vital functions, potentially causing delays in critical operations, inaccurate readings, or even complete shutdowns of battery systems.

(ii) *Ransomware Attacks:* Ransomware attacks can severely compromise the availability of a battery system by encrypting critical system files and demanding a ransom for their release [95]. In such attacks, malicious software infiltrates the BMS infrastructure through various entry points, exploiting vulnerabilities or utilizing social engineering tactics. Once inside, the ransomware encrypts essential files and data necessary for the operation of the BMS, effectively locking out legitimate users and administrators. This encryption renders the system inaccessible and disrupts its ability to monitor and control battery health and performance. Consequently, the BMS may fail to provide accurate readings, trigger false alarms, or even halt critical operations altogether. Given the vital role of battery systems, such attacks can have far-reaching consequences, including safety risks, operational disruptions, and financial losses.

(iii) *Application Level Battery Draining Attacks:* As battery systems should function in the context of applications, the intrusions or abuse at the application level may excessively deplete the battery power. For example, malicious malware can break into the telematic system of EVs, execute unnecessary tasks in the background, or execute resource-intensive tasks without consent from users. As a result, the batteries of these devices are depleted at an accelerated rate, potentially leading to unexpected shutdowns or failures. Moreover, the diminished battery life of these devices can compromise the effectiveness of the BMS, hindering its ability to accurately monitor and manage battery health and performance. We highlight multiple instances of such attacks in ❸ ***Real-world Examples*** to provide readers with more insights.

(iv) *Cyberattacks on Charging Infrastructure:* Although this paper focuses mainly on the security and assurance of the battery system itself, cyberattacks on their accessories like charging infrastructure have implications affecting the availability of corresponding battery-operated applications. For example, charging stations provide a convenient and accessible infrastructure for EV owners to recharge their vehicles. However, as networked equipment, cybersecurity breaches are unsurprisingly witnessed, e.g., in 2018, by gaining access to the connected WiFI, Kaspersky Lab researchers found a way to (1) stop the charging processor or (2) set the charger to the maximum current possible [96]. In the (1) scenario, EV drivers may have to call tow trucks if nearby charging stations are down because of cyberattacks. As for (2), compromised charging stations could output current pulses to intentionally damage the battery systems. Similarly, in 2021, Schneider Electric, a major vendor of EV charging stations, announced new patches against several new vulnerabilities that could allow adversaries to tamper with the charging station's settings and accounts [97].

❸ ***Real-world Examples:*** Intelligent adversaries have developed a variety of methods to violate the availability of batteries, e.g., battery-draining attacks. For instance, *Polite WiFi* attack was proposed in [18] where the researchers identified a vulnerability in the WiFi protocol, i.e., all WiFi devices acknowledge *any* received frame if the destination address points to their MAC address. In other words, even a packet with invalid content (fake packet) will also trigger the response from the device with WiFi. As seen in Fig. 10(a), a victim laptop is connected to an access point within a private WiFi network whereas it would respond to fake packets from attackers. Such blind physical layer acknowledgments may result in quite a few negative impacts including battery-draining attacks. An adversary can intentionally flood fake packet streams to force the acknowledgment behaviors from victim devices. [18] has identified this can accelerate the battery-draining procedure of low-power IoT devices by `35x`, which can reduce the lifetime of sensitive applications such as sensors or medical devices significantly.

The availability of battery systems in EVs can be compromised by battery-draining attacks as well. [93] investigated the operation modes, e.g., normal and sleep, of the electronic control units (ECUs), which is a core control system of most modern EVs. They discovered that injecting the *wake-up* message to the in-vehicle network (e.g., CAN bus) can effectively prevent EVs from entering the energy-saving mode as seen in Fig. 10(b). The experimental results on test vehicles demonstrate a `12.57x` increase in terms of the average battery power consumption; the battery of a parked car can be drained within only a few days or even hours. Another real-world example of battery-draining attacks in EVs is [98] where adversaries target Nissan Leaf, a popular series of EVs. Specifically, they managed to exploit vulnerable APIs of the smartphone app of the EVs to enable them to connect and *control* any Nissan Leaf vehicle (also its BMS) of the same fleet by sending maliciously crafted packets. The intrusions stealthily drain the battery energy because attackers can even remotely turn the air conditioner (AC) on. Such hacking forced Nissan to suspend their app for threat mitigation immediately [99] and release corresponding software security patches later for affected vehicles [100].

In addition to dedicated attacks on BMS itself, it is worth noting that subverting the application level could also lead to battery availability issues as attackers may intentionally enable power-intensive features like AC, car audio, and light systems. In 2022, it was reported that security specialists broke into the telematics systems of 25 Tesla vehicles across 13 countries by remotely gaining very high privileges including checking if a driver is present in the car, turning on the stereo sound systems, and flashing headlights [101], implying excessive consumption of battery energy. Besides, back in 2015, two hackers exploited software flaws in Jeep Cherokee and further silently rewrote the firmware of underlying chips such that malicious commands could reach physical components through the in-vehicle CAN bus. Battery energy can be quickly drained here by letting the car blast cloud air at the maximum setting and play music at full volume [102].

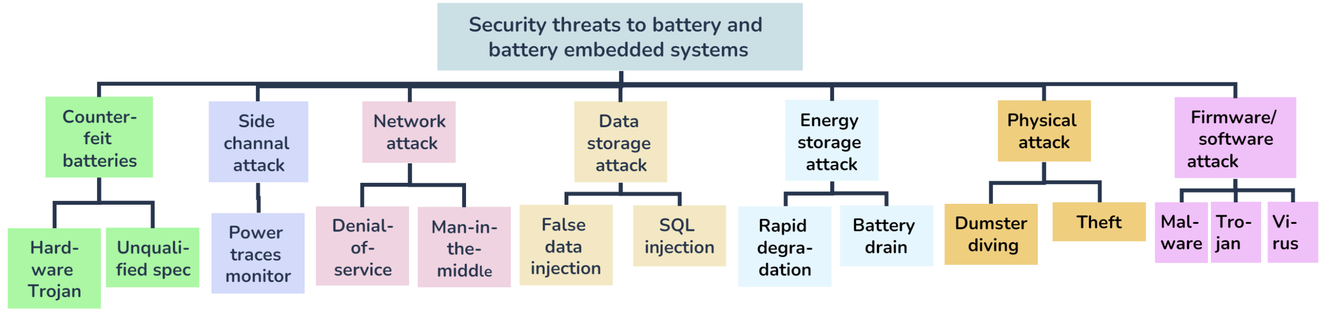


Fig. 11. Taxonomy of security threats to battery and battery embedded systems [26, 103–105].

TABLE VI
ATTACKS ON BATTERY.

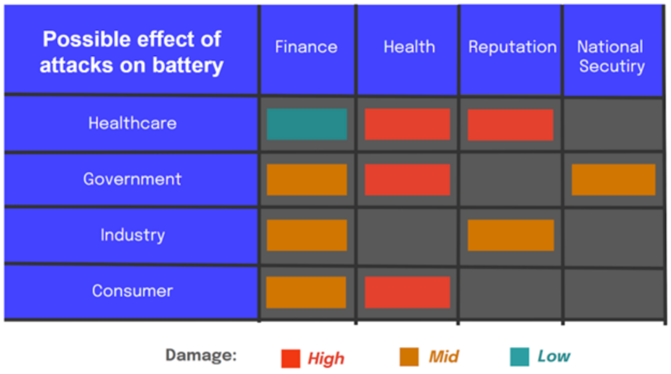
Attack Vectors	**Type of Attacks**	**Attack Scenario**	**Impact**	**Severity**
False data injection	Cyber	Malware, Trojan, virus or physical access	Misjudging the state of the battery by the controller or user	★ ★ ★
SQL injection	Cyber	The attacker interferes the database with SQL queries	Information leakage	★
Denial of service	Cyber	Overloading either the physical or network connections	The battery system can no longer be accessed	★ ★
Man in the middle	Cyber	Using a hacker to change the communication between entitles who think they are directly communicating with each other	Information leakage, unauthorized operation, installation of malware, Trojan or virus	★ ★ ★
Rapid degradation	Cyber	Compromise system estimation, making the battery keep overcharge or over-discharge	Degradation of the capacity of the battery or even explosion	★ ★ ★
Battery drain	Cyber	Bombarding the victim with fake packets, to which the battery system will keep sending ACKs back	Fasten the drainage of the battery	★
Malware, Trojan, and Virus	Cyber	Phishing emails, social engineering, or through the use of infected USB drives	Data theft, system failure, or damage to the batteries	★ ★ ★
Side channel attack	Cyber	Malicious batteries (compromised or counterfeit) analyze the side channel info of the device	Information leakage	★
Chemical Alteration attack	Physical	Malicious batteries (Impure chemicals are injected instead of original material) analyze the side channel info of the device	Low quality, low capacity or degraded battery	★ ★ ★
Mislabeling	Physical	Original label of the battery and casings are replaced with fake ones to show them as better quality battery	Misrepresented, low capacity battery, fire safety issues	★ ★ ★
Counterfeiting	Physical	Original battery specifications are altered, bad components are injected	Degraded, low capacity battery, fire safety issues	★ ★ ★

C. Summary and Perspectives of Security Threats

In this subsection, we would like to summarize and highlight the major attack vectors that would affect battery security. We cover not only the attack vectors threatening BMS assurance but also a few supply chain attack vectors on battery authenticity to make the summary comprehensive. Note that most of them have been detailed in Section II-B and Section III-B whereas we would like to summarize them horizontally in terms of attack characteristics, make the information more accessible, and present our additional perspectives.

Fig. 11 depicts the taxonomy of security threats to battery and battery-embedded systems and Table VI summarizes our point of view on the detailed attack scenario and impact of the attacks with their corresponding severity. as detailed follows.

1) *Network Attack:* This type of attack aims at the communication channel between the battery and the controller or between the battery system and the user. The attacker could be overloading the physical or network connections to perform a DOS attack to make the battery or the entire system unavailable, or use a hacker to change the communication between entitles who think they are directly communicating with each other to breach the stored data or perform unauthorized operations like installing malware/Trojan/virus [106, 107].
2) *Data Storage Attack:* This type of attack aims at the data storage unit of the battery system. The attacker tries to either alter or breach the data stored in the battery system using various methods including malware, Trojan, virus, physical access, or interfering with the database with SQL queries [108].
3) *Energy Storage Attack:* This type of attack aims at the energy storage unit of the battery system. The attacker tries to drain the energy of the battery by bombarding the victim with fake packets, to which the battery system will keep responding with ACK signals, or cause the capacity of the battery to rapidly degrade by injecting false data into the battery state estimation, which would make the controller wrongly estimate the state of the battery and keeps overly charging or discharging the battery [109].
4) *Physical Attack:* This type of attack aims at the physical access of the battery system by either theft or dumpster diving, which could lead to various problems like information leakage and reverse engineering [104]. Nowadays, the BMS is designed specifically for the applications and hence are customized [110]. Reverse engineering of such BMS can lead the adversary to get complete access to the architecture of the BMS, further leading to realizing the security vulnerabilities and even theft of the BMS IP design [19]. Moreover, physical fault injection attacks are dangerous. For example, an external EM source can induce a large Eddy current into the on-chip power distribution network to disturb the BMS circuitry by causing setup/hold time violations in a contactless manner.
5) *Firmware/Software Attack:* This type of attack aims at the firmware or software of the battery-embedded system. The attacker could install malware, Trojans, or viruses to the battery system through phishing emails,



Possible effect of attacks on battery	Finance	Health	Reputation	National Secutiry
Healthcare	🟦	🟥	🟥	
Government	🟧	🟥		🟧
Industry	🟧		🟧	
Consumer	🟧	🟥		

Damage: 🟥 High 🟧 Mid 🟦 Low

Fig. 12. Perspectives on impacts of attacks on batteries in primary sectors.

social engineering, or the use of infected USB drives, which could cause problems like data theft, system failure, or damage to the batteries [111].

6) *Counterfeit Batteries:* Counterfeit batteries usually do not have the same specs as legitimate batteries. They may have low capacity, short life spec, or even a lack of safety parts, which makes them physically dangerous. Also, there could be some malicious hardware Trojan installed in the counterfeit batteries, which could lead to more serious problems [112].
7) *Side-Channel Attack:* Researchers have discovered that a malicious battery can obtain (steal) various types of information from a device by analyzing its side channel information, e.g., continuously monitoring power traces [113]. By analyzing the power traces of a battery, the activity of the battery-powered system can be predicted [114]. For example, tracing the power consumption of a cell phone can lead to realizing the usage and type of usage as well [115].

Fig. 12 shows our perspective on the possible effects of attacked or counterfeit batteries on various sectors. Attacks on battery systems can affect almost all industrial sectors financially. Besides, loss of lives is mostly caused by failures of battery systems in healthcare, government, and consumer electronics. Moreover, the most critical property of a healthcare enterprise is its reputation. Battery-induced issues in their products could easily destroy a huge business. Finally, a malfunction of military equipment controlled by the government leads to a serious concens on national security.

IV. State-of-the-art Battery Security Solutions

There have been existing solutions aiming to enhance both battery system authenticity and assurance. In this section, we will first discuss state-of-the-art battery authenticity solutions with a focus on counterfeit battery detection. Next, solutions for ensuring BMS assurance are presented.

A. State-of-the-art Battery Authenticity Solutions

Existing methods of battery authentication are extensively used to distinguish original batteries and counterfeit or low-quality substitutes. Visual inspection, chemical analysis, form factor, and the resistance of the target battery instance, as well as several challenge-response mechanisms, are used to distinguish original and fake batteries.

TABLE VII
State-of-the-art methods of battery authentication [112].

Methods	Cloning	Replay	Unscalability	Rewrapping
Markings	No	Yes	Yes	No
External Factors	No	Yes	Yes	No
Form Factor	No	Yes	Yes	No
Resistor	No	Yes	Yes	No
Chip	Yes	No	No	No
DCAuth [112]	Yes	Yes	Yes	Yes
EISthentication [112]	Yes	Yes	Yes	Yes

1) *Visual Inspection:* Visual inspection involves looking for physical characteristics that are unique to the manufacturer or product and using them to detect. Markings, logos, or labels on the battery, its color, shape, and size can be used in the inspection process to detect authenticity [116–119]. This method, however, is vulnerable to deliberate rewrapping attacks, and in general, it is easy to replicate the markings on the wrapping or other external characteristics.
2) *Form Factor:* Form factors are related to the form of a battery. A battery's form factor refers to its size, configuration, and arrangement. The three most common form factors for EV batteries are cylindrical, prismatic, and pouch. [120].
3) *Resistor of Battery:* Using resistance for battery authentication has two aspects: Placing an external resistance inside the battery or using the internal resistance as an identifier. However, externally placed batteries can be extracted and placed inside a counterfeit one to make it look like an original battery [112]. Using internal resistance has also some limitations as the resistance of a Li-ion battery does not always stay constant during all states of operation as seen in Fig. 13.
4) *Challenge response protocol:* Challenge-Response (CR) protocol between the chip and the prover can be used to validate the battery. One implementation of this protocol is using an unchanging stream of bits that, however, can be sniffed by an attacker and thus is vulnerable to replay attacks. More advanced gauges instead include some cryptographic hash function in the protocol, making it impossible for an attacker to steal the authentication codes.
5) *Emerging Technologies:* [112] presents two novel methodologies, namely, *DCAuth* and *EISthentication*. Both of them leverage the internal characteristics of each battery cell using ML methods. The training data comes from the regular usage of Li-ion battery models including only physical and chemical features. More specifically, *DCAuth* and *EISthentication* require only voltage and capacity measurements (i.e., differential capacity analysis data) and electrochemical impedance spectroscopy data, respectively. The solutions can achieve up to 0.94 accuracy in counterfeit battery detection [112].

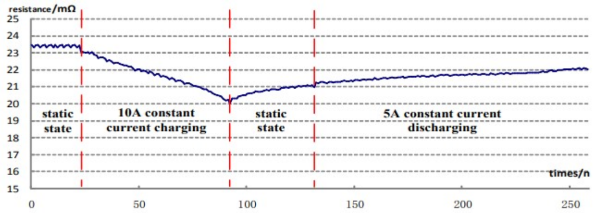


Fig. 13. Internal resistance change curve in the charging-discharging process of batteries [121].

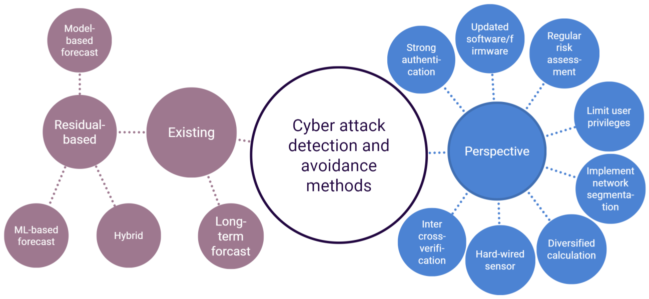


Fig. 14. Cyber attack detection and avoidance methods [103–105, 130, 132, 133].

B. State-of-the-art Battery Assurance Methods

As shown in Fig. 14, the existing detection methods mostly fall into three categories: residual-based forecasting, long-term forecasting, and hybrid methods [103].

- *Residual-based methods* forecasts the system's behavior either using models or machine learning methods and compares the forecasted value and the measured value to see if there are differences notable enough to indicate potential cyber attacks [122]. The performance of a residual-based detector is intricately tied to the accuracy of the forecasting technique employed, which ensures that deviations between predicted and observed values are accurately identified, leading to more robust anomaly detection in the BESS system. Consequently, selecting a forecasting method with exceptionally high accuracy is crucial when dealing with Battery Energy Storage System (BESS)-related datasets.
  (i) Model-based methods: Two prevalent methods are *Coulomb Counting* [123, 124] and equivalent circuit models (ECMs) [125]. However, both methods come with notable limitations [126]. Coulomb counting relies on precise initial cell state data, and its accuracy is susceptible to meter errors and model inaccuracies [127]. Meanwhile, ECMs, despite their utility, overlook certain physiochemical processes occurring within the battery cell and demand detailed empirical parameterization for their application [128].
  (ii) Machine learning based methods: Several types of classifiers find application in forecasting the battery system behaviors, including artificial neural networks (ANNs) with feed-forward Neural Networks (NNs), recurrent NNs, which are suitable for sequential data processing, and deep NNs (e.g., Deep Belief NN), as well as fuzzy logic and its combination with NN (an adaptive neuro-fuzzy inference system), and other combined machine learning methods [129].
  (iii) Hybrid methods: The combination of Machine Learning based methods with model-based approaches results in a class of hybrid methods. This integration leverages the strengths of both methods, utilizing the data-driven capabilities of ML alongside the structured understanding provided by model-based techniques. Hybrid methods often demonstrate improved performance and versatility [130].
- *Long-term forecasting methods* create typical profiles for system behaviors and compare the general features periodically to see whether there is potentially altered data. This could resolve the limitation of the residual-based methods that the forecast value may be inaccurate, leveraging the fact that cyber attacks usually need to be effective for a long period to cause significant damages. However, this method may struggle to detect or respond effectively to sudden and rapid cyber attacks. Forecasting the consumption by clustering typical load profiles is a typical approach for behavior forecasting in the electric grid domain [131], where probabilistic neural networks (PNNs) are applied for consumer clustering, dividing consumers into clusters based on the load profiles to obtain a typical load profile.

V. Perspective Battery Security Solutions

Although quite a few contemporary solutions are discussed in Section IV, they may not completely address the complicated battery security model. Therefore, in this section, we would like to present our perspectives on some possible and promising methods to provide insightful directions that the research community can look into.

A. Perspective Battery Authenticity Methods

We provision three perspective methods for ensuring battery authenticity. The first one is battery physical unclonable function (PUF) which aims to fingerprint each battery instance. The other two refer to blockchain and zero-trust architecture for battery supply chain management to enhance its resilience and transparency.

1) Potential Battery PUF: PUF was originally proposed to uniquely fingerprint each IC by characterizing the process variations of silicon [134]. Similarly, battery authenticity can significantly benefit from such implementation to identify counterfeit instances. Internal parameters of batteries are of paramount importance in building a universal identification (ID) for batteries. At the cell level, the variation of internal parameters arises from the diverse structure of anode, cathode, and electrolytes.

a) Characterzing the Internal Parameters of Li-ion Batteries: The most practiced internal parameters of battery are: pressure drop between two sides of the battery [135], internal resistance (IR) [136], batteries natural frequency [137], temperature pattern [138], open circuit voltage (OCV) [139], etc.

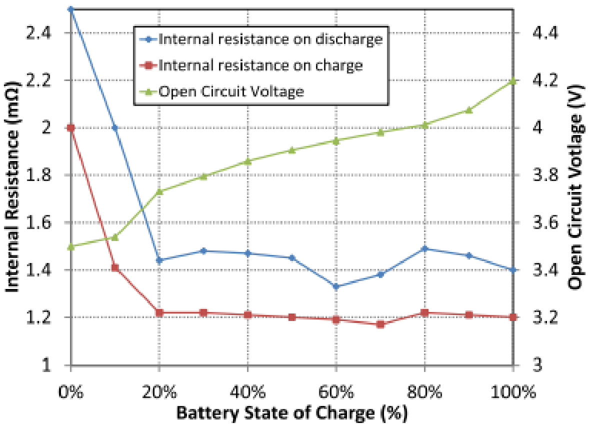


Fig. 15. Internal resistance variation of a Nissan leaf battery cell.

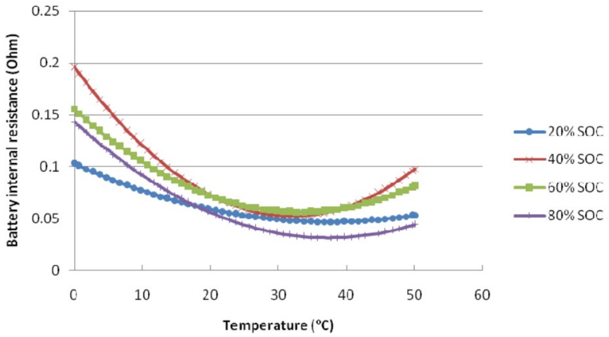


Fig. 16. Battery internal resistance as a function of both temperature and SoC.

As all of these parameters are interrelated, only one needs to be chosen carefully so that the usual characteristics of that parameter do not change much with time. Primarily, we propose the internal resistance of the battery as a potential parameter for battery PUF design. The internal resistance of a battery is a function of different parameters, including current, voltage, state of charge, state of health, battery natural frequency, etc. [140]. The dependency of internal resistance on different parameters has been shown in Fig. 15 and Fig. 16. Fig. 15 shows the measurement data of open circuit voltage, and internal resistances on charging and discharging for a Nissan Leaf battery cell [141]. Based on Fig. 16, it can be concluded that the minimum battery internal resistance will be between 20C to 40C as can be observed from the trend of the graphs [142].

Fig. 13 shows the internal resistance change curve of a certain brand of two 5Ah lithium iron phosphate batteries in the charging-discharging process [121]. The charge preparation process, which is the stage where the battery is not being charged or discharged is static, and the internal resistance is stable. The maximum rate of change of resistance is 0.61% in this state. In the charge state, a significant amount of lithium-ions strip from the cathode and enter into the electrolyte because of the increase in the electrochemical activity of the battery. The resistance towards the current of the battery is reduced and the internal resistance presents a decreasing tendency. The internal resistance reduces by 12.3% post charging as compared to the value before charging [143]. After charging the battery stays in a static state, while the internal resistance of the battery rises gradually. However, the rate of increase becomes slower in this state. The internal resistance remains unchanged after the value reaches 21.1 $m\Omega$. Subsequently, in the discharging process, the battery has a 1C constant current meaning that a fully charged battery rated at 1Ah should provide 1A for one hour, and the internal resistance of the battery increases slowly.

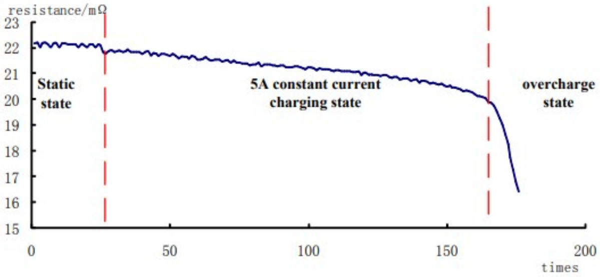


Fig. 17. The internal resistance change curve in the overcharging process of batteries [143].

At the initial static state, the internal resistance of the battery is stable and decreases at the 1C constant current charging stage. When the battery reaches the upper cut-off voltage and gets into the overcharge state, the decreased speed of internal resistance amplifies suddenly as shown in Fig. 17 [143]. According to this characteristic of Li-ion battery, it is difficult to detect the overcharge fault of the battery and to predict the same [144].

From the literature it is evident that internal resistance can efficiently indicate the battery's SoH [145, 146], SoC [147], and can also monitor thermal runaway [148, 149]. The detection of internal resistance improves the accuracy of battery inconsistency diagnosis. Because the internal resistance of the battery truly reflects its properties, detecting variations in internal resistance improves the accuracy of possible malicious detection and also forecasts battery failure. Furthermore, in EVs, the IR gives critical information about regenerative braking capabilities, dynamic charge and discharge efficiency, and battery physical degradation[150]. Therefore, the IR must be assessed in order to characterize the performance of an EV battery system. The IR is an important battery parameter since it is closely related to its power output, energy efficiency, ability to perform quick charging and regenerative braking, and physical cell degradation [151]. All of these characteristics are critical for the efficient operation of a battery-powered application, making IR a candidate worth exploring for developing a PUF for battery systems.

b) Perspective PUF Design for Battery Systems: As mentioned, a PUF [152, 153] is a hardware security primitive that exploits the unique and unpredictable variations in physical characteristics of a device to generate a unique identifier or a cryptographic key [154–156]. PUFs can be classified based on different criteria, such as their operating principle, the type of physical variations they exploit, and the type of output they produce [157]. In recent years, it has come to be recognized as the digital fingerprint; it is as unique as human fingerprints[134, 158]. PUF's one-of-a-kind quality distinguishes it as a potential technique for key generation, identification, and authentication difficulties. Because of their low power consumption, small footprint, and resilience to physical and side-channel assaults, PUFs have emerged as a promising alternative for increasing the security of devices.

As discussed above, IR is one of the most essential properties of a battery since it is used to evaluate power performance [159], energy efficiency [150], aging mechanisms [160], and equivalent circuit modeling [161]. In addition, as shown in the previous section, a potential malicious attack can have a substantial impact on IR properties, proving its capability to be used as a parameter for a PUF design in batteries. We propose a method to authenticate the life cycle of batteries by considering the internal resistance values during different processes. The created PUF identifier can be saved as a physical tag on top of the battery or in the battery management system's memory.

c) Proposed Methodology: The energy storage system, which charges and releases energy from a battery, is directly affected by battery performance; hence, a BMS that manages, protects, and interacts with the outside world is essential. One of the issues with nonlinear batteries is that their internal features vary as the quantity of charge-discharge cycles increases; hence, the primary purpose of a BMS is to precisely track these changes. Based on the decline in efficiency (which occurs during battery use), our approach will provide a way to enhance the security of batteries and efficiency by using a battery efficiency equation and applying it to calculate and predict the SoC and SoH of the battery. The internal resistance of a battery is the key indicator of its state. The internal resistance of a battery increases with an increase in the heat generated during the charge-discharge of the battery. This approach will help monitor the battery state and prevent it from overcharging and over-discharging, improving its security and performance.

d) Proposed Architecture: Our proposed method's technological implementation is based on signed battery data, using keys extracted from the battery's PUF. The most functional part of our method will involve updating and adding the data of the battery especially its internal resistance as it changes along the battery life period. In our approach, every new data generated will be sent to the central database of each battery. Only the signature is appended to a battery-specific certificate that also includes the public key. If a certificate for the battery already exists, it must be reissued, and the previous one has to be voided. The proposed architecture will hereby include three steps in general: 1) Update of battery records 2) Verification that certificate belongs to records 3) Verify that battery belongs to the certificate. One of the advantages of this architecture is that the derived key may be stored in a security module like BMS to avoid the risk of stolen or reproduced keys by a malicious identity. Our future work will include a detailed architecture with the experimental results of this approach. Our work will also include developing potential sensors to detect any kind of malicious attacks or counterfeiting relating the sensors to the battery PUFs.

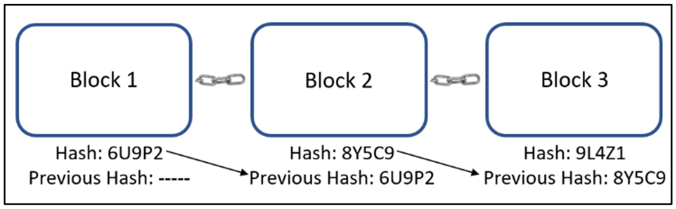


Fig. 18. The blockchain architecture.

2) Blockchain for Battery Supply Chain: Blockchain has emerged as a popular technology in supply chain management like food, logistics, and microelectronics. Similarly, we see its great potential to enhance the authenticity of the battery supply chain as proposed below.

a) Blockchain in Supply Chain Management: Blockchain technology, functions as a distributed database and a peer-to-peer network that stores a registry of transactions [162]. Initially developed for cryptocurrencies, blockchain offers various features, including decentralization, immutability, traceability, trust, and transparency [162–164]. These features have contributed to the widespread adoption of blockchain in diverse fields, such as online voting, banking, and the Internet of Things [165]. Extending its applications, blockchain's implementation for Web3 is currently trending. Using blockchain for Web3, a newer and better internet managed by users, is increasing trust amongst the users [166]. In a blockchain, each block can be likened to a folder on a computer (node) that contains specific data. The blockchain itself comprises these interconnected sub-folders [167]. Fig. 18 illustrates the structure of a blockchain, wherein each block is linked to its preceding block through a hash. Blockchain is categorized into different types based on two factors: the type of ownership and the level of access granted to participants.

- *Public Blockchain:* This type of blockchain is an open blockchain, where participation is unrestricted, and anyone can join the network at any time [168].
- *Private Blockchain:* This network is one where a single entity operates and runs the blockchain. In this type of blockchain, ownership is concentrated in the hands of one party, unlike the public blockchain. Consequently, it does not possess the full decentralization characteristic typically associated with blockchain networks [169].
- *Consortium Blockchain:* In this blockchain, multiple parties are granted permissioned control over the entire network, distinguishing it from the previously described types. This blockchain is characterized by a fair and transparent decision-making process, contributing to smooth operations. Additionally, it offers reduced costs and increased efficiency compared to other models [170]. For the purpose of this investigation, a consortium blockchain is utilized [171].

The smart contract plays a pivotal role in blockchain technology and is vital for establishing trust within the network [172]. Despite its name, the smart contract does not have a legal context and is simply a computer program [173]. The code of the smart contract is stored on the blockchain and is linked to a unique address [174]. In adherence to the terms

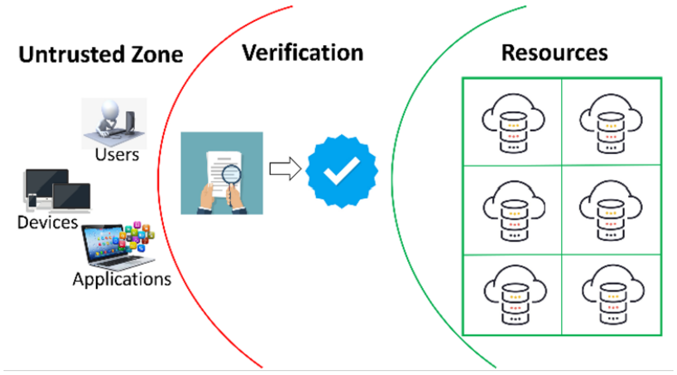


Fig. 19. A zero trust access model.

TABLE VIII
ZERO TRUST TENETS AND THEIR INTERPRETATION.

Tenets	**Interpretation**
Data and computation are considered as resources	Disparate resource set
Information is secured regardless of location	Independent security
Access to resources on a per-session basis	Traceability
Access is determined by a dynamic policy Provenance	Provenance
Device and assets are held in the most secure state possible Confidentiality	Confidentiality
Authentication and authorization are strictly enforced Integrity	Integrity
Collection of information on current state to improve security Persistent Evaluation	Persistent Evaluation

defined by the smart contract, any updates made within the blockchain network are considered valid only when a majority of the involved parties reach an agreement or consensus. If a consensus is not achieved, the update is deemed invalid and consequently rejected [175]. Blockchain technology has been investigated extensively to answer crucial challenges like tracking and tracing of varied products in the supply chain including food and agriculture [176], pharma[177]. In addition, the use of physical unclonable functions (PUFs) in union with blockchain is found in the semiconductor supply chain [40, 178–182].

b) Perspective Methodology: We postulate innovative solutions to safeguard the integrity and authenticity of batteries throughout the supply chain using a combination of Unique Identifiers (UIDs) and blockchain technology. The potential battery PUF discussed in Section V-A1, is the Unique Identifier we propose to use. This approach would help in addressing the pressing concern of counterfeiting and tampering within the battery supply chain, which can lead to significant reliability and safety risks. By embedding PUFs within batteries, unique identifiers are generated, serving as immutable identifiers of authenticity. These identifiers are then securely stored on a blockchain, creating a transparent and auditable ledger of battery provenance. Through this integration of UIDs and blockchain, stakeholders can verify the authenticity of batteries at each stage of the supply chain, mitigating the threat of counterfeit or compromised products. The consortium blockchain ensures accountability and traceability, enabling swift identification of malicious actors and compromised batteries. In essence, the combination of UIDs and blockchain technology offers a holistic solution to the multifaceted challenges facing the battery supply chain, providing a robust framework for ensuring trust, transparency, and integrity from manufacturing to deployment.

TABLE IX
SUMMARY OF ZERO TRUST POLICIES AND IMPLEMENTATIONS.

Policies	**Implementation**	**Feature utilized**
Disparate resource set	Multifactor Authentication	Blockchain/Unique ID
Independent security	Modifier function of smart contract	Blockchain/Unique ID
Traceability	Traceability feature of blockchain	Blockchain
Provenance	Provenance check feature of blockchain	Blockchain
Confidentiality	Modifiers in smart contract	Blockchain
Integrity	Immutability feature of blockchain	Blockchain
Persistent Evaluation	Monitoring the blockchain	Blockchain

3) Zero Trust Architecture for Battery Supply Chain:

Zero trust is a security concept that challenges the traditional notion of trust and assumes the potential presence of an attacker within the network [183], [184]. It operates on the fundamental principle that nothing in the network should be automatically trusted without proper verification. In accordance with NIST SP 800-207 [184], a cybersecurity plan that incorporates the principles of zero trust, encompassing the management of component relationships, workflow planning, and access policies, is referred to as a zero trust architecture (ZTA).

The term zero trust was first introduced in 2010 by the analyst firm Forrester Research to address modern attacks in the information security domain [185], [186]. In the traditional security model, everything within the security boundaries is assumed to be trusted. However, with recent advances in technology, this assumption has become obsolete [187]. Zero trust is a cybersecurity paradigm that concentrates on resource protection and acknowledges that trust cannot be blindly placed in anything but must be continually evaluated [184, 185], [187]. It is centered on the belief that organizations should not automatically trust anything inside or outside their periphery. Instead, every access request and connection attempt should be verified before granting access. This leads to micro-segmentation of the network which is the foundation of a zero trust network as illustrated in Fig. 19.

In practice, the concept of zero trust entails that access to any resource within the network must adhere to predefined trust dimensions or parameters. Failure to meet these parameters should result in the denial or revocation of access to the specific resource [188]. Zero trust encompasses a set of concepts and ideas aimed at reducing uncertainty in enforcing precise, least-privilege, and per-request access decisions in information systems and services. This approach leads to the creation of a micro-segmented network [189].

Based on this principle, the National Institute of Standards and Technology (NIST) has defined seven tenets that characterize zero trust in a special publication [184]. These tenets are as follows.

- Data and computation are considered as resources.
- Information is secured regardless of location.
- Access to resources on a per-session basis.
- Access is determined by a dynamic policy.
- Device and assets are held in the most secure state possible.
- Authentication and authorization are strictly enforced.
- Collection of information on current state to improve security

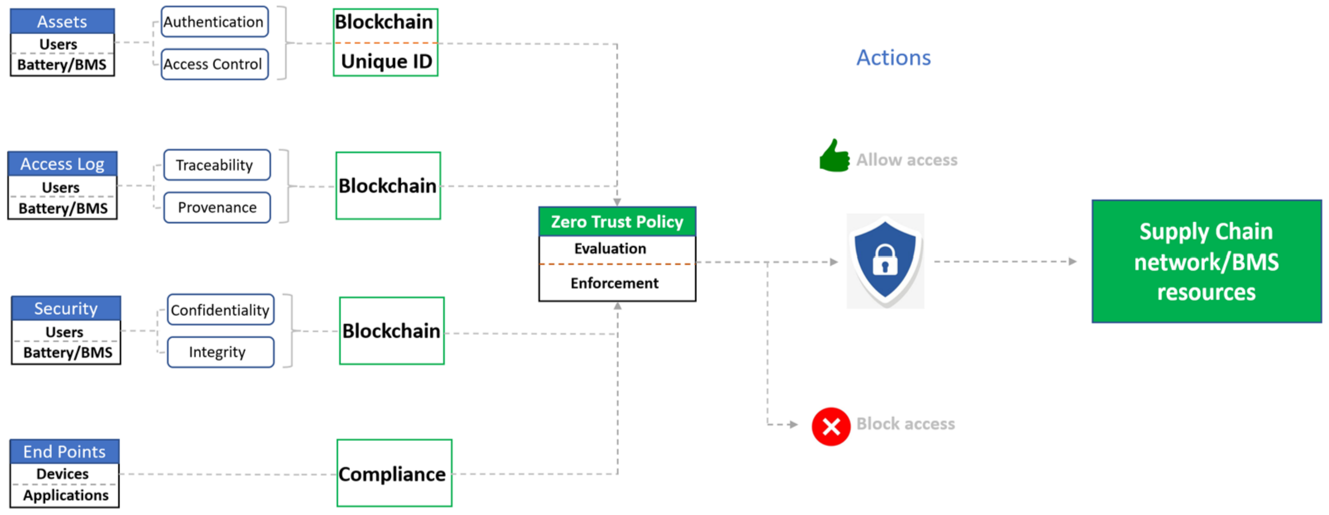


Fig. 20. Proposed zero trust architecture for battery security.

These above tenets can be applied to the battery supply chain. Moreover, policies for access control and authentication can be formulated to enhance the security and integrity of the supply chain ecosystem. In the proposed model, all transactions taking place within the network are recorded in the blockchain, ensuring a transparent and immutable record of actions. This recording of transactions serves to track the sequence of events and maintain accountability within the network.

a) Proposed Architecture: To achieve a successful implementation of a zero trust architecture, it is essential to adhere to the tenets outlined by NIST, which establish a secure perimeter around the supply chain network. These tenets focus on access control, authorization, supervision, and overall security. For user authorization, blockchain technology is primarily utilized, leveraging its features such as transparency and decentralized control. Unique identifiers such as battery PUFs can play a crucial role in authenticating the battery and/or battery system within the network. The tenets are interpreted specifically for the battery supply chain domain and are presented in Table VIII.

The proposed zero trust architecture for the battery supply chain, as depicted in Fig. 20, integrates various components and mechanisms to ensure authentication, access control, traceability, and security. The authentication and access control of the users is mainly done through a blockchain-enabled MFA and battery/BMS is authenticated via unique identifiers. The transactions performed in the network are updated on the shared blockchain ledger and hence are trackable and traceable. To maintain the confidentiality and integrity of the assets, features offered by blockchain are utilized. Furthermore, this work enforces that all the devices used in the network are updated with the latest security patches and all the computer codes are developed taking into consideration the concepts of secure coding, thus adhering to the ZT compliance. The zero trust policy engine evaluates and enforces all the policies formulated for the architecture. Upon enforcement of the protocols, access to the network resources is either allowed or blocked, depending upon the evaluation of the policies laid and their implementation. With these protocols in place, everything that enters the network to fetch access to the resources is verified and authenticated, with very little or no room for an untrusted element to enter the network.

All these policies have been formulated based on the principles laid down by NIST and are summarized in Table IX.

B. Perspective Battery Assurance Methods

As shown in Fig. 14, the potential avoidance methods include strong authentication, updated software/firmware, regular risk assessment, limited user privileges, implementation of network segmentation, diversified calculation, hard-wired sensor, and inter cross-verification [104, 105].

- *Strong Authentication:* As discussed in previous sections, an attacker can get access to the battery system through methods like guessing passwords or social engineering, which can be mitigated by strong authentications like complicated passwords or multi-step verification.
- *Updated Software/Firmware:* As mentioned in previous sections, the software or firmware on the battery system can be the target of an attacker, so keeping them updated constantly can effectively reduce the chance of them being altered by the opponents, leading to the compromise of the entire system.
- *Limited User Privileges:* In addition to the above techniques, limiting the privileges for users is also very useful in terms of preventing unauthorized operations like installing malware/Trojan from being performed on the battery system even when the outer authentication of the battery system is cracked by the attacker.
- *Implementation of Network Segmentation:* As demonstrated in previous sections, cyber attacks can be aimed at the networking of the battery system, so commonly used network security techniques like the implementation of network segmentation, which divides a network into

smaller, distinct sub-networks and enable network teams to separate the sub-networks and deliver unique security controls and services to each sub-network, can be used to effectively reduce the chance of the networking system of the battery system being compromised.
- *Regular Risk Assessment:* Just like any other rising technology, the security issues that the battery systems are facing are evolving dramatically every day, hence it is crucial to maintain regular risk assessment to keep the battery system up to the latest challenges.
- *Diversified Calculation:* Another potential mitigation strategy for safeguarding against the compromise of state estimation calculations is diversifying the calculation methods and their execution locations within the battery management system for cross-verification [132].
- *Hard-wired Sensor:* Certain hard-wired sensors could be potentially considered as safety triggers (e.g. temperature and current sensors). There could be designed responses to certain abnormal incidents such as immediate shutdown or backing off the stages [133].
- *Inter Cross-verification:* Considering the interconnection of modern BMSs, cyber attack detection methods like residual-based methods and long-term forecasting methods could be applied with cross-verification among different BMSs to enhance accuracy and prevent unauthorized modification to the detection module.

Given the complexity of such issues, we understand that neither the state-of-the-art nor our perspective solutions can be sliver bullets to guarantee battery security from now on. However, we hope the insights provided in this **INSPECT** paper can shed some light on the problem landscape and pave the way for future research efforts.

VI. Conclusion

It is universally acknowledged that the concerns around batteries are serious, calling for scrutinization and deliberation. In this paper, we abandon outdated beliefs that battery manufacturers are the major entities who are responsible for the ramifications. The state-of-the-art attack vectors that can violate the critical properties, i.e., authenticity and assurance, of prevalent Li-ion battery packs are reviewed comprehensively. Also, we strive to figure out the potentially feasible solutions to mitigate the security problems of battery packs such as countermeasures against cyber-physical attack vectors, battery PUF, and zero-trust platforms for battery supply chain. With this perspective paper, we would like to raise the attention of both industry and academia, leading to new research directions and promising methodologies ensuring battery security in the new era.

References

[1] Statista Research Department. Size of the global battery market from 2018 to 2021, with a forecast through 2030, by technology. https://www.statista.com/statistics/1339880/global-battery-market-size-by-technology/. Online.

[2] Precedence Research. Battery market size to be worth around usd 475.37 bn by 2032. https://www.globenewswire.com/en/news-release/2023/07/07/2701036/0/en/Battery-Market-Size-to-be-Worth-Around-USD-475-37-Bn-by-2032.html. Online.

[3] Los Angeles Field Office. Counterfeit and substandard lithium (cr123a) power cell batteries pose serious health and safety risks to law enforcement officers, other consumers. https://info.publicintelligence.net/FBI-LithiumBatteries.pdf. Online, posted on 7 June 2012.

[4] Gilberto Garcia-Vazquez. The electronics industry's counterfeit parts problem. https://www.macrofab.com/blog/electronics-industry-counterfeit-parts-problem/#:~:text=For%20example%2C%20in%202016%20a,sales%20hovered%20around%20$5%20billion. Online.

[5] Christine Torralba. Busting the myth: Yes, cell phones can explode. https://www.androidauthority.com/busting-the-myth-yes-cell-phones-can-explode-42582/. Online, posted on January 8, 2012.

[6] Tim Moynihan. Why hoverboards keep exploding. https://www.wired.com/2015/12/why-hoverboards-keep-exploding/. Online, posted on DEC 12, 2015.

[7] The counterfeit report. United flight downed by fraudulent li-ion battery pack. https://thecounterfeitreport.com/press_release_details.php?date=2020-03-12&id=888. Online, posted on March 12, 2020.

[8] April Rubin. Lithium-ion batteries in e-bikes and other devices pose fire risks. https://www.nytimes.com/2022/11/14/us/lithium-ion-ebike-battery-fires.html. Online, posted on Nov. 15, 2022.

[9] Namu Sampath. Video: Brockton house catches fire twice in one night, sparked by lithium-ion batteries. https://www.enterprisenews.com/story/news/fire/2023/01/06/brockton-house-fire-168-bartlett-street-lithium-ion-batteries-scooter/69784329007/. Online, posted on Jane 7, 2023.

[10] CarsDover. How many electric cars catch fire every year. https://www.carjunkya.com/electric-car-fire-statistics/. Online, posted on June 26, 2023.

[11] Qingsong Wang, Binbin Mao, Stanislav I. Stoliarov, and Jinhua Sun. A review of lithium ion battery failure mechanisms and fire prevention strategies. *Progress in Energy and Combustion Science*, 73:95–131, 2019.

[12] US immigration and customs enforcement. Former simi valley ceo convicted of selling navy knock-off batteries used on subs and aircraft carriers. https://www.reuters.com/article/us-usa-california-fraud-idUSKCN0I52NF20141016/. Online.

[13] Cbp seizes counterfeit hoverboards with potentially dangerous batteries. https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-counterfeit-hoverboards-potentially-dangerous-batteries. Online.

[14] Ice hsi arrests chinese national in $23.8 million scheme to sell counterfeit laptop computer batteries on ebay and amazon. https://m.facebook.com/wwwICEgov/posts/d41d8cd9/10157663040446815/?locale=zh_CN. Online.

[15] Latham company pays $75000 for selling counterfeit battery. https://www.justice.gov/usao-ndny/pr/latham-company-pays-75000-selling-counterfeit-batteries-department-defense. Online.

[16] Ziad M. Ali, Martin Calasan, Foad H. Gandoman, Francisco Jurado, and Shady H.E. Abdel Aleem. Review of batteries reliability in electric vehicle and e-mobility applications. *Ain Shams Engineering Journal*, 15(2):102442, 2024.

[17] Analog Devices Inc. Battery Management Systems (BMS). https://www.analog.com/en/applications/markets/automotive-pavilion-home/electrification-and-powertrain/battery-management-systems-bms.html.

[18] Ali Abedi and Omid Abari. Wifi says" hi!" back to strangers! In *Proceedings of the 19th ACM Workshop on Hot Topics in Networks*, pages 132–138, 2020.

[19] Patrick Kiley. Reverse Engineering the Tesla Battery Management System to Increase Power Available. https://www.youtube.com/watch?v=UV2zvgyIF0I.

[20] Partha P Paul, Eric J McShane, Andrew M Colclasure, Nitash Balsara, David E Brown, Chuntian Cao, Bor-Rong Chen,

Parameswara R Chinnam, Yi Cui, Eric J Dufek, et al. A review of existing and emerging methods for lithium detection and characterization in li-ion and li-metal batteries. *Advanced Energy Materials*, 11(17):2100372, 2021.

[21] Lingxi Kong, Diganta Das, and Michael G Pecht. The distribution and detection issues of counterfeit lithium-ion batteries. *Energies*, 15(10):3798, 2022.

[22] Khurum Nazir Junejo and Jonathan Goh. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In *Proceedings of the 2nd ACM international workshop on cyber-physical system security*, pages 34–43, 2016.

[23] Hyunjun Lee, Gomanth Bere, Kyungtak Kim, Justin J Ochoa, Joung-hu Park, and Taesic Kim. Deep learning-based false sensor data detection for battery energy storage systems. In *2020 IEEE CyberPELS (CyberPELS)*, pages 1–6. IEEE, 2020.

[24] Nitin Varshney, Haoting Shen, Olivia Paradis, and Navid Asadizanjani. He-ion beam imaging for accurate hardware trojan detection. *Microscopy and Microanalysis*, 26(S2):188–190, 2020.

[25] Mark M Tehranipoor, Navid Asadi-Zanjani, Olivia Pauline Paradis, and Nitin Varshney. Hardware deprocessing using voltage imaging for hardware assurance, March 14 2023. US Patent 11,604,912.

[26] Eduard Kovacs. Mobile devices exposed to spying via malicious batteries: Researchers. https://www.securityweek.com/mobile-devices-exposed-spying-malicious-batteries-researchers/#:~:text=Researchers%20from%20Technion%2C%20UT%20Austin,the%20most%20information%2C%20experts%20said. Online, posted on June 25, 2018.

[27] Ning Wen, Jian Wang, and Tao Zhang. Hardware trojan detection technique based on som neural network. In *2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, pages 1645–1648. IEEE, 2018.

[28] Minyan Gao, M Sazadur Rahman, Nitin Varshney, Mark Tehranipoor, and Domenic Forte. iprobe: Internal shielding approach for protecting against front-side and back-side probing attacks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2023.

[29] Sazadur Rahman, Nitin Varshney, Farimah Farahmandi, Navid Asadi Zanjani, and Mark Tehranipoor. Lle: Mitigating ic piracy and reverse engineering by last level edit. In *ISTFA 2023*, pages 360–369. ASM International, 2023.

[30] Tasnuva Farheen, Ulbert Botero, Nitin Varshney, Damon L Woodard, Mark Tehranipoor, Domenic Forte, and Haoting Shen. Proof of reverse engineering barrier: sem image analysis on covert gates. In *ISTFA 2021*, pages 179–189. ASM International, 2021.

[31] Olivia P Dizon-Paradis, Nitin Varshney, M Tanjidur Rahman, Michael Strizich, Haoting Shen, and Navid Asadizanjani. Insitu thickness measurement of die silicon using voltage imaging for hardware assurance. *arXiv preprint arXiv:2307.13118*, 2023.

[32] Jorge A Llamas-Orozco, Fanran Meng, Gavin S Walker, Amir F N Abdul-Manan, Heather L MacLean, I Daniel Posen, and Jon McKechnie. Estimating the environmental impacts of global lithium-ion battery supply chain: A temporal, geographical, and technological perspective. *PNAS Nexus*, 2(11):pgad361, 11 2023.

[33] Becky Chapman. How does a lithium-Ion battery work? https://www.analog.com/en/applications/markets/automotive-pavilion-home/electrification-and-powertrain/battery-management-systems-bms.html.

[34] MATLAB. What is battery pack design? *Mathworks MATLAB*.

[35] Jiangyun Zhang, Xinxi Li, Fengqi He, Jieshan He, Zhaoda Zhong, and Guoqing Zhang. Experimental investigation on thermal management of electric vehicle battery module with paraffin/expanded graphite composite phase change material. *International Journal of Photoenergy*, 2017:1–8, 12 2017.

[36] Elias Ribeiro da Silva, Jacob Lohmer, Michelle Rohla, and Jannis Angelis. Unleashing the circular economy in the electric vehicle battery supply chain: A case study on data sharing and blockchain potential. *Resources, Conservation and Recycling*, 193:106969, 2023.

[37] Elsa A. Olivetti, Gerbrand Ceder, Gabrielle G. Gaustad, and Xinkai Fu. Lithium-ion battery supply chain considerations: Analysis of potential bottlenecks in critical metals. *Joule*, 1(2):229–243, 2017.

[38] Yangtao Liu, Ruihan Zhang, Jun Wang, and Yan Wang. Current and future lithium-ion battery manufacturing. *iScience*, 24(4):102332, 2021.

[39] Zhongbao Wei, Jiyun Zhao, Hongwen He, Guanglin Ding, Haoyong Cui, and Longcheng Liu. Future smart battery and management: Advanced sensing from external to embedded multi-dimensional measurement. *Journal of Power Sources*, 489:229462, 2021.

[40] Tao Zhang, Fahim Rahman, Mark Tehranipoor, and Farimah Farahmandi. Fpga-chain: Enabling holistic protection of fpga supply chain with blockchain technology. *IEEE Design & Test*, 40(2):127–136, 2022.

[41] Rouhan Noor, Himanandhan Reddy Kottur, Patrick J Craig, Liton Kumar Biswas, M Shafkat M Khan, Nitin Varshney, Hamed Dalir, Elif Akçalı, Bahar Motlagh, Charles Woychik, et al. Us microelectronics packaging ecosystem: Challenges and opportunities. *arXiv preprint arXiv:2310.11651*, 2023.

[42] Aida Damanpak Rizi, Antika Roy, Rouhan Noor, Hyo Kang, Nitin Varshney, Katja Jacob, Sindia Rivera-Jimenez, Nathan Edwards, Volker J Sorger, Hamed Dalir, et al. From talent shortage to workforce excellence in the chips act era: Harnessing industry 4.0 paradigms for a sustainable future in domestic chip production. *arXiv preprint arXiv:2308.00215*, 2023.

[43] PC magazine. Chasing black mass: Inside the electric vehicle battery recycling process.

[44] Alessandra R. Carreon. The ev battery supply chain explained. *RMI*.

[45] Diganta Das Lingxi Kong and Michael G. Pecht. The distribution and detection issues of counterfeit lithium-ion batteries. *Molecular Diversity Preservation International*, 2022.

[46] L Gaines and R Cuenca. Costs of lithium-ion batteries for vehicles. 8 2000.

[47] International energy agency. The pitfalls of buying lithium batteries. *Energetech Solar*.

[48] Kae E. Fink, Bryant J. Polzin, John T. Vaughey, Joshua J. Major, Alison R. Dunlop, Stephen E. Trask, Gerald T. Jeka, Jeffrey S. Spangenberger, and Matthew A. Keyser. Influence of metallic contaminants on the electrochemical and thermal behavior of li-ion electrodes. *Journal of Power Sources*, 518:230760, 2022.

[49] He Liu, Xinbing Cheng, Yan Chong, Hong Yuan, Jia-Qi Huang, and Qiang Zhang. Advanced electrode processing of lithium ion batteries: A review of powder technology in battery fabrication. *Particuology*, 57:56–71, 2021.

[50] Aluminium insider. Cmitsubishi materials co. reveals falsified quality data for aluminium products. *Aluminium insider*.

[51] Underwriters Laboratories. Counterfeit lithium-ion cells and batteries. *UL*.

[52] Gary Hunt et al. Usabc electric vehicle battery test procedures manual. *United States Department of Energy: Washington, DC, USA*, 1996.

[53] Lingxi Kong, Diganta Das, and Michael G. Pecht. The distribution and detection issues of counterfeit lithium-ion batteries. *Energies*, 15(10), 2022.

[54] Tapesh Joshi, Saad Azam, Daniel Juarez-Robles, and Judith A Jeevarajan. Safety and quality issues of counterfeit lithium-ion cells. *ACS energy letters*, 8:2831–2839, 2023.

[55] The Counterfeit Report. How to identify counterfeit lithium

ion 18650 batteries. *The Counterfeit Report*.

[56] Energy5. Understanding the risks of counterfeit batteries. *Energy5*.

[57] Hayley B Potts. Woman burned by exploding e-cigarette battery awarded $1.9m. *LA Times*.

[58] Farshid Naseri, Zahra Kazemi, Peter Gorm Larsen, Mohammad Mehdi Arefi, and Erik Schaltz. Cyber-physical cloud battery management systems: Review of security aspects. *Batteries*, 9(7):382, 2023.

[59] BOSCH. Battery in the Cloud. https://www.bosch-mobility.com/en/solutions/software-and-services/battery-in-the-cloud/battery-in-the-cloud/.

[60] Weihan Li, Monika Rentemeister, Julia Badeda, Dominik Jöst, Dominik Schulte, and Dirk Uwe Sauer. Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation. *Journal of energy storage*, 30:101557, 2020.

[61] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18(3):2027–2051, 2016.

[62] William G Halfond, Jeremy Viegas, Alessandro Orso, et al. A classification of sql-injection attacks and countermeasures. In *Proceedings of the IEEE international symposium on secure software engineering*, volume 1, pages 13–15. IEEE, 2006.

[63] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, pages 1093–1110, 2017.

[64] Chris Eagle. *The IDA pro book*. no starch press, 2011.

[65] Chris Eagle and Kara Nance. *The Ghidra Book: The Definitive Guide*. no starch press, 2020.

[66] Tao Zhang, Jian Wang, Shize Guo, and Zhe Chen. A comprehensive fpga reverse engineering tool-chain: From bitstream to rtl code. *IEEE Access*, 7:38379–38389, 2019.

[67] Tao Zhang, Mark Tehranipoor, and Farimah Farahmandi. Bitfree: On significant speedup and security applications of fpga bitstream format reverse engineering. In *2023 IEEE European Test Symposium (ETS)*, pages 1–6. IEEE, 2023.

[68] Tao Zhang, Jian Wang, and Zhe Chen. A reverse engineering-based framework assisting hardware trojan detection for encrypted ips. In *2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, pages 1649–1652. IEEE, 2018.

[69] Zheng Ding, Qiang Wu, Yizhong Zhang, and Linjie Zhu. Deriving an ncd file from an fpga bitstream: Methodology, architecture and evaluation. *Microprocessors and Microsystems*, 37(3):299–312, 2013.

[70] Marc Fyrbiak, Sebastian Strauß, Christian Kison, Sebastian Wallat, Malte Elson, Nikol Rummel, and Christof Paar. Hardware reverse engineering: Overview and open challenges. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pages 88–94. IEEE, 2017.

[71] Shahed E Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. A survey on chip to system reverse engineering. *ACM journal on emerging technologies in computing systems (JETC)*, 13(1):1–34, 2016.

[72] Tao Zhang, Jungmin Park, Mark Tehranipoor, and Farimah Farahmandi. Psc-tg: Rtl power side-channel leakage assessment with test pattern generation. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pages 709–714. IEEE, 2021.

[73] Ashwin Chandwani, Saikat Dey, and Ayan Mallik. Cybersecurity of onboard charging systems for electric vehicles—review, challenges and countermeasures. *IEEE Access*, 8:226982–226998, 2020.

[74] Stephen M Trimberger and Jason J Moore. Fpga security: Motivations, features, and applications. *Proceedings of the IEEE*, 102(8):1248–1265, 2014.

[75] Mark Zhao and G Edward Suh. Fpga-based remote power side-channel attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 229–244. IEEE, 2018.

[76] Łukasz Olejnik, Gunes Acar, Claude Castelluccia, and Claudia Diaz. The leaking battery: A privacy analysis of the html5 battery status api. In *Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, September 21–22, 2015. Revised Selected Papers 10*, pages 254–263. Springer, 2016.

[77] Taesic Kim, Justin Ochoa, Tasnimun Faika, H Alan Mantooth, Jia Di, Qinghua Li, and Young Lee. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 10(1):1270–1281, 2020.

[78] Adam Duncan, Adib Nahiyan, Fahim Rahman, Grant Skipper, Martin Swany, Andrew Lukefahr, Farimah Farahmandi, and Mark Tehranipoor. Serfi: secure remote fpga initialization in an untrusted environment. In *2020 IEEE 38th VLSI Test Symposium (VTS)*, pages 1–6. IEEE, 2020.

[79] Pawel Swierczynski, Georg T Becker, Amir Moradi, and Christof Paar. Bitstream fault injections (bifi)–automated fault attacks against sram-based fpgas. *IEEE Transactions on Computers*, 67(3):348–360, 2017.

[80] Maik Ender, Amir Moradi, and Christof Paar. The unpatchable silicon: a full break of the bitstream encryption of xilinx 7-series {FPGAs}. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1803–1819, 2020.

[81] Tao Zhang, Md Latifur Rahman, Hadi Mardani Kamali, Kimia Zamiri Azar, Mark Tehranipoor, and Farimah Farahmandi. Fishi: Fault injection detection in secure heterogeneous integration via power noise variation. In *2023 IEEE 73rd Electronic Components and Technology Conference (ECTC)*, pages 2188–2195. IEEE, 2023.

[82] Amit Mazumder Shuvo, Tao Zhang, Farimah Farahmandi, and Mark Tehranipoor. A comprehensive survey on non-invasive fault injection attacks. *Cryptology ePrint Archive*, 2023.

[83] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE design & test of computers*, 27(1):10–25, 2010.

[84] Kan Xiao, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22(1):1–23, 2016.

[85] Swarup Bhunia and Mark M Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.

[86] Nidish Vashistha, Hangwei Lu, Qihang Shi, M Tanjidur Rahman, Haoting Shen, Damon L Woodard, Navid Asadizanjani, and Mark Tehranipoor. Trojan scanner: Detecting hardware trojans with rapid sem imaging combined with image processing and machine learning. In *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*, page 256. ASM International, 2018.

[87] Adib Nahiyan, Mehdi Sadi, Rahul Vittal, Gustavo Contreras, Domenic Forte, and Mark Tehranipoor. Hardware trojan detection through information flow security verification. In *2017 IEEE International Test Conference (ITC)*, pages 1–10. IEEE, 2017.

[88] Tao Zhang, Md Latifur Rahman, Hadi Mardani Kamali, Kimia Zamiri Azar, and Farimah Farahmandi. Sipguard: Run-time system-in-package security monitoring via power noise variation. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2023.

[89] Nitin Varshney, Chengjie Xi, Aslam A Khan, Liton Kumar Biswas, Volker Sorger, Hamed Dalir, and Navid Asadizanjani. Electron beam probing: The new sheriff in town for security analyzing of sub-7nm ics-exploring the advantages of a post-

photon emission technique. In *ISTFA 2023*, pages 346–351. ASM International, 2023.

[90] Hyo Jin Jo, Jin Hyun Kim, Hyon-Young Choi, Wonsuk Choi, Dong Hoon Lee, and Insup Lee. Mauth-can: Masquerade-attack-proof authentication for in-vehicle networks. *IEEE transactions on vehicular technology*, 69(2):2204–2218, 2019.

[91] Khalid Mahmood Malik, Hafiz Malik, and Roland Baumann. Towards vulnerability analysis of voice-driven interfaces and countermeasures for replay attacks. In *2019 IEEE conference on multimedia information processing and retrieval (MIPR)*, pages 523–528. IEEE, 2019.

[92] Charlie Miller. Battery firmware hacking. *Black Hat USA*, pages 3–4, 2011.

[93] Kyong-Tak Cho, Yuseung Kim, and Kang G Shin. Who killed my parked car? *arXiv preprint arXiv:1801.07741*, 2018.

[94] Meiko Jensen, Nils Gruschka, and Norbert Luttenberger. The impact of flooding attacks on network-based services. In *2008 Third International Conference on Availability, Reliability and Security*, pages 509–513. IEEE, 2008.

[95] Tao Zhang, Mark Tehranipoor, and Farimah Farahmandi. Trustguard: Standalone fpga-based security monitoring through power side-channel. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2023.

[96] Kaspersky Lab. Vulnerabilities in Connected Electric Car Chargers Could Damage Home Networks. https://www.kaspersky.com/about/press-releases/2018_vulnerabilities-in-connected-electric-car-chargers-could-damage-home-networks.

[97] Eduard Kovacs. New Flaws Expose EVlink Electric Vehicle Charging Stations to Remote Hacking. https://www.securityweek.com/new-flaws-expose-evlink-electric-vehicle-charging-stations-remote-hacking/.

[98] Troy Hunt. Controlling Vehicle Features of Nissan LEAFs across the Globe via Vulnerable APIs. https://www.troyhunt.com/controlling-vehicle-features-of-nissan/.

[99] BBC News. Nissan Disables Leaf App after Car Hack Risk Revealed Online. https://www.bbc.com/news/technology-35660641.

[100] Mahmoud Hashem Eiza and Qiang Ni. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, 12(2):45–51, 2017.

[101] Bussiness Insider. A 19-year-old Security Researcher Describes How He Remotely Hacked into over 25 Teslas. https://www.businessinsider.com/teen-security-researcher-describes-how-he-hacked-into-25-teslas-2022-1.

[102] WIRED. Hackers Remotely Kill a Jeep on the Highway. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[103] Nina Kharlamova, Chresten Træhold, and Seyedmostafa Hashemi. Cyberattack detection methods for battery energy storage systems. *Journal of Energy Storage*, 69:107795, 2023.

[104] Taesic Kim, Justin Ochoa, Tasnimun Faika, H. Alan Mantooth, Jia Di, Qinghua Li, and Young Lee. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 10(1):1270–1281, 2022.

[105] Gopal Krishna, Rajesh Singh, Anita Gehlot, Nagendar Yamsani, Samta Kathuria, and Shaik Vaseem Akram. Enhancing the cyber-security of battery management systems for energy storage. In *2023 IEEE World Conference on Applied Intelligence and Computing (AIC)*, pages 959–964, 2023.

[106] Marco Pasetti, Paolo Ferrari, Paolo Bellagente, Emiliano Sisinni, Alan Oliveira de Sá, Charles B. do Prado, Rodrigo P. David, and Raphael Carlos Santos Machado. Artificial neural network-based stealth attack on battery energy storage systems. *IEEE Transactions on Smart Grid*, 12(6):5310–5321, 2021.

[107] T. Martin, M. Hsiao, Dong Ha, and J. Krishnaswami. Denial-of-service attacks on battery-powered mobile computers. In *Second IEEE Annual Conference on Pervasive Computing and Communications, 2004. Proceedings of the*, pages 309–318, 2004.

[108] Peng Zhuang and Hao Liang. False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks. *IEEE Transactions on Smart Grid*, 12(3):2566–2577, 2021.

[109] Haijun Ruan, Jingyi Chen, Weilong Ai, and Billy Wu. Generalised diagnostic framework for rapid battery degradation quantification with deep learning. *Energy and AI*, 9:100158, 2022.

[110] EPEC. Custom BMS VS. Off-the-shelf BMS: Features and Limitations. https://blog.epectec.com/custom-bms-vs-off-the-shelf-bms-features-and-limitations.

[111] Anthony Bahadir Lopez, Korosh Vatanparvar, Atul Prasad Deb Nath, Shuo Yang, Swarup Bhunia, and Mohammad Abdullah Al Faruque. A security perspective on battery systems of the internet of things. *Journal of Hardware and Systems Security*, 1:188–199, 2017.

[112] Mauro Conti Francesco Marchiori. Your battery is a blast! safeguarding against counterfeit batteries with authentication. https://dl.acm.org/doi/abs/10.1145/3576915.3623179. Online.

[113] Rowshon Munny and John Hu. Power side-channel attack detection through battery impedance monitoring. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5, 2021.

[114] Lide Zhang, Birjodh Tiwana, Robert P. Dick, Zhiyun Qian, Z. Morley Mao, Zhaoguang Wang, and Lei Yang. Accurate online power estimation and automatic battery behavior based power model generation for smartphones. In *2010 IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, pages 105–114, 2010.

[115] Qing Yang, Paolo Gasti, Gang Zhou, Aydin Farajidavar, and Kiran S. Balagani. On inferring browsing activity on smartphones via usb power analysis side-channel. *IEEE Transactions on Information Forensics and Security*, 12(5):1056–1066, 2017.

[116] Shajib Ghosh, Patrick Craig, Jake Julia, Nitin Varshney, Hamed Dalir, and Navid Asadizanjani. Deepiclogo: A novel benchmark dataset for deep learning-based ic logo detection. In *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pages 1–8. IEEE, 2023.

[117] Navid Asadizanjani, Mir Tanjidur Rahman, Mark Tehranipoor, Navid Asadizanjani, Mir Tanjidur Rahman, and Mark Tehranipoor. Counterfeit detection and avoidance with physical inspection. *Physical Assurance: For Electronic Devices and Systems*, pages 21–47, 2021.

[118] Mark Tehranipoor, N Nalla Anandakumar, and Farimah Farahmandi. Recycled fpga detection. In *Hardware Security Training, Hands-on!*, pages 53–72. Springer, 2023.

[119] Mark Tehranipoor, Nitin Pundir, Nidish Vashistha, and Farimah Farahmandi. Counterfeit and recycled ic detection. In *Hardware Security Primitives*, pages 281–300. Springer, 2022.

[120] DIYGuru. Different Form Factors of EV Battery. https://diyguru.org/automotive/different-form-factors-of-ev-battery-2/#:~:text=The%20form%20factor%20of%20an,types%20of%20EVs%20and%20applications.

[121] Dian Wang, Yun Bao, and Jianjun Shi. Online lithium-ion battery internal resistance measurement application in state-of-charge estimation using the extended kalman filter. *Energies*, 10(9), 2017.

[122] Sungwoo Cho, Hyeonseok Jeong, Chonghun Han, Shanshan Jin, Jae Hwan Lim, and Jeonkeun Oh. State-of-charge estimation for lithium-ion batteries under various operating conditions using an equivalent circuit model. *Computers & Chemical Engineering*, 41:1–9, 2012.

[123] Jeong Lee and Jehyuk Won. Enhanced coulomb counting method for soc and soh estimation based on coulombic efficiency. *IEEE Access*, 11:15449–15459, 2023.

[124] Wen-Yeau Chang. The state of charge estimating methods for

battery: A review. *ISRN Applied Mathematics*, 2013, 01 2013.

[125] Guangming Liu, Languang Lu, Hong Fu, Jianfeng Hua, Jianqiu Li, Minggao Ouyang, Yanjing Wang, Shan Xue, and Ping Chen. A comparative study of equivalent circuit models and enhanced equivalent circuit models of lithium-ion batteries with different model structures. In *2014 IEEE Conference and Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific)*, pages 1–6, 2014.

[126] Giovanni Nobile, Ester Vasta, Mario Cacciato, Giuseppe Scarcella, and Giacomo Scelba. Estimation of soh for battery packs: A real-time mixed algorithm based on coulomb counting method and parameter-varying circuit modeling. In *2020 IEEE 11th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, pages 536–541, 2020.

[127] Kiarash Movassagh, Sheikh Arif Raihan, Balakumar Balasingam, and Krishna Pattipati. A critical look at coulomb counting approach for state of charge estimation in batteries. *Energies*, 14:4074, 07 2021.

[128] Zhongbao Wei, Rui Xiong, Tuti Mariana Lim, Shujuan Meng, and Maria Skyllas-Kazacos. Online monitoring of state of charge and capacity loss for vanadium redox flow battery based on autoregressive exogenous modeling. *Journal of Power Sources*, 402:252–262, 2018.

[129] M.S. Hossain Lipu, M.A. Hannan, Aini Hussain, Afida Ayob, Mohamad H.M. Saad, Tahia F. Karim, and Dickson N.T. How. Data-driven state of charge estimation of lithium-ion batteries: Algorithms, implementation factors, limitations and future trends. *Journal of Cleaner Production*, 277:124110, 2020.

[130] Manjot S. Sidhu, Deepak Ronanki, and Sheldon Williamson. State of charge estimation of lithium-ion batteries using hybrid machine learning technique. In *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, volume 1, pages 2732–2737, 2019.

[131] D. Gerbec, S. Gasperic, I. Smon, and F. Gubina. Allocation of the load profiles to consumers using probabilistic neural networks. *IEEE Transactions on Power Systems*, 20(2):548–555, 2005.

[132] Madeline CHEAH* et.al. Feature Article: Cybersecurity of Battery Management Systems. https://www.horiba.com/int/company/news/detail/news/10/2019/feature-article-cybersecurity-of-battery-management-systems/.

[133] Wei Wei Kong, Yugong Luo, Yunlong Qi, and Yongsheng Wang. Full protection scheme and energy optimization management of the battery in internal combustion engine vehicles based on power partitioning model. Technical report, SAE Technical Paper, 2019.

[134] Wenjie Che, Fareena Saqib, and Jim Plusquellic. Puf-based authentication. In *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 337–344. IEEE, 2015.

[135] Ao Tang, Jie Bao, and Maria Skyllas-Kazacos. Studies on pressure losses and flow rate optimization in vanadium redox flow battery. *Journal of power sources*, 248:154–162, 2014.

[136] Ashok K Singal. The internal resistance of a battery. *arXiv preprint arXiv:1308.4913*, 2013.

[137] Hongwen He, Rui Xiong, and Hongqiang Guo. Online estimation of model parameters and state-of-charge of lifepo4 batteries in electric vehicles. *Applied Energy*, 89(1):413–420, 2012.

[138] Valerie H Johnson, Ahmad A Pesaran, and Thomas Sack. Temperature-dependent battery models for high-power lithium-ion batteries. Technical report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2001.

[139] B Pattipati, B Balasingam, GV Avvari, Krishna R Pattipati, and Y Bar-Shalom. Open circuit voltage characterization of lithium-ion batteries. *Journal of Power Sources*, 269:317–333, 2014.

[140] Julian Blümke and Hans-Joachim Hof. Authentic batteries: A concept for a battery pass based on puf-enabled certificates. In *SECURWARE 2022: The Sixteenth International Conference on Emerging Security Information, Systems and Technologies*, pages 76–81. International Academy, Research and Industry Association (IARIA), 2022.

[141] Samveg Saxena, Caroline Le Floch, Jason MacDonald, and Scott Moura. Quantifying ev battery end-of-life through analysis of travel needs with vehicle powertrain models. *Journal of Power Sources*, 282:265–276, 2015.

[142] Amirul Haniff Mahmud, Zul Hilmi Che Daud, and Zainab Asus. The impact of battery operating temperature and state of charge on the lithium-ion battery internal resistance. 2017.

[143] Hua Zhang, Rengui Lu, Chunbo Zhu, and Yongping Zhao. Online measurement of internal resistance of lithium ion battery for ev and its application research. *International Journal of u-and e-Service, Science and Technology*, 7(4):301–310, 2014.

[144] Manh-Kien Tran and Michael Fowler. A review of lithium-ion battery fault diagnostic algorithms: Current progress and future challenges. *Algorithms*, 13(3):62, 2020.

[145] P. Singh and D. Reisner. Fuzzy logic-based state-of-health determination of lead acid batteries. In *24th Annual International Telecommunications Energy Conference*, pages 583–590, 2002.

[146] Pritpal Singh, Ramana Vinjamuri, Xiquan Wang, and David Reisner. Design and implementation of a fuzzy logic-based state-of-charge meter for Li-ion batteries used in portable defibrillators. *Journal of Power Sources*, 162(2):829–836, January 2006.

[147] Mohammad A Hannan, MS Hossain Lipu, Aini Hussain, and Azah Mohamed. A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: Challenges and recommendations. *Renewable and Sustainable Energy Reviews*, 78:834–854, 2017.

[148] Shalini Rodrigues, Nookala Munichandraiah, and Arun Kumar Shukla. Ac impedance and state-of-charge analysis of a sealed lithium-ion rechargeable battery. *Journal of Solid State Electrochemistry*, 3:397–405, 1999.

[149] I Uchida, H Ishikawa, M Mohamedi, and M Umeda. Ac-impedance measurements during thermal runaway process in several lithium/polymer batteries. *Journal of power sources*, 119:821–825, 2003.

[150] David Ansean, Manuela Gonzalez, Juan Carlos Viera, Victor Manuel Garcia, Juan Carlos Alvarez, and Cecilio Blanco. Electric vehicle li-ion battery evaluation based on internal resistance analysis. In *2014 IEEE Vehicle Power and Propulsion Conference (VPPC)*, pages 1–6, 2014.

[151] Jeong Lee, Jun-Mo Kim, Junsin Yi, and Chung-Yuen Won. Battery management system algorithm for energy storage systems considering battery efficiency. *Electronics*, 10(15):1859, 2021.

[152] Mark Tehranipoor, N Nalla Anandakumar, and Farimah Farahmandi. Physical unclonable functions (pufs). In *Hardware Security Training, Hands-on!*, pages 1–17. Springer, 2023.

[153] Mark Tehranipoor, Nitin Pundir, Nidish Vashistha, and Farimah Farahmandi. Volatile memory-based puf. In *Hardware Security Primitives*, pages 49–62. Springer, 2022.

[154] Muslim Mustapa. *PUF based FPGAs for hardware security and trust*. PhD thesis, University of Toledo, 2015.

[155] Basel Halak, Mark Zwolinski, and M Syafiq Mispan. Overview of puf-based hardware security solutions for the internet of things. In *2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4. IEEE, 2016.

[156] Fatemeh Ganji, Shahin Tajik, Jean-Pierre Seifert, Domenic Forte, and Mark M Tehranipoor. Hardness amplification of physical unclonable functions (pufs), October 24 2023. US Patent 11,799,673.

[157] Mark Tehranipoor, Nitin Pundir, Nidish Vashistha, and Farimah Farahmandi. Intrinsic-transient puf. In *Hardware*

Security Primitives, pages 17–32. Springer, 2022.

[158] Thomas McGrath, Ibrahim E Bagci, Zhiming M Wang, Utz Roedig, and Robert J Young. A puf taxonomy. *Applied physics reviews*, 6(1), 2019.

[159] Xiaosong Hu, Rui Xiong, and Bo Egardt. Model-based dynamic power assessment of lithium-ion batteries considering different operating conditions. *IEEE Transactions on Industrial Informatics*, 10(3):1948–1959, 2013.

[160] Elixabete Sarasketa-Zabala, Egoitz Martinez-Laserna, Maitane Berecibar, Inigo Gandiaga, Lide Mercedes Rodriguez-Martinez, and Igor Villarreal. Realistic lifetime prediction approach for li-ion batteries. *Applied energy*, 162:839–852, 2016.

[161] Fouad Eltoumi, Adberrezak Badji, Mohamed Becherif, and HS Ramadan. Experimental identification using equivalent circuit model for lithium-ion battery. *International Journal of Emerging Electric Power Systems*, 19(3):20170210, 2018.

[162] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008.

[163] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, and Minho Jo. A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. *IEEE Access*, 8:88700–88716, 2020.

[164] Abirami Raja Santhi and Padmakumar Muthuswamy. Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics*, 6(1):15, 2022.

[165] Marco Iansiti, Karim R Lakhani, et al. The truth about blockchain. *Harvard business review*, 95(1):118–127, 2017.

[166] Ahto Buldas, Dirk Draheim, Mike Gault, Risto Laanoja, Takehiko Nagumo, Märt Saarepera, Syed Attique Shah, Joosep Simm, Jamie Steiner, Tanel Tammet, et al. An ultra-scalable blockchain platform for universal asset tokenization: design and implementation. *IEEE Access*, 10:77284–77322, 2022.

[167] Akshay Kulkarni, Noor Ahmad Hazari, and Mohammed Niamat. A blockchain technology approach for the security and trust of the ic supply chain. In *2019 IEEE National Aerospace and Electronics Conference (NAECON)*, pages 249–252. IEEE, 2019.

[168] Felix Irresberger, Kose John, Peter Mueller, and Fahad Saleh. The public blockchain ecosystem: An empirical analysis. *NYU Stern School of Business*, 2021.

[169] Sunny Pahlajani, Avinash Kshirsagar, and Vinod Pachghare. Survey on private blockchain consensus algorithms. In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, pages 1–6. IEEE, 2019.

[170] Mingxiao Du, Qijun Chen, Jieying Chen, and Xiaofeng Ma. An optimized consortium blockchain for medical information sharing. *IEEE Transactions on Engineering Management*, 68(6):1677–1689, 2020.

[171] Jiawen Kang, Rong Yu, Xumin Huang, Sabita Maharjan, Yan Zhang, and Ekram Hossain. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE transactions on industrial informatics*, 13(6):3154–3164, 2017.

[172] Daniel Macrinici, Cristian Cartofeanu, and Shang Gao. Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8):2337–2354, 2018.

[173] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20*, pages 79–94. Springer, 2016.

[174] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 254–269, 2016.

[175] Weizhi Meng, Elmar Wolfgang Tischhauser, Qingju Wang, Yu Wang, and Jinguang Han. When intrusion detection meets blockchain technology: a review. *Ieee Access*, 6:10179–10188, 2018.

[176] Feng Tian. An agri-food supply chain traceability system for china based on rfid & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)*, pages 1–6. IEEE, 2016.

[177] Gaurav Kumar Badhotiya, Vijay Prakash Sharma, Surya Prakash, Vinayak Kalluri, and Ranbir Singh. Investigation and assessment of blockchain technology adoption in the pharmaceutical supply chain. *Materials Today: Proceedings*, 46:10776–10780, 2021.

[178] Xiaolin Xu, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. Electronics supply chain integrity enabled by blockchain. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 24(3):1–25, 2019.

[179] Jason Vosatka, Andrew Stern, MM Hossain, Fahim Rahman, Jeffery Allen, Monica Allen, Farimah Farahmandi, and Mark Tehranipoor. Tracking cloned electronic components using a consortium-based blockchain infrastructure. In *2020 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pages 1–6. IEEE, 2020.

[180] Fahim Rahman and Mark Tehranipoor. Blockchain-enabled electronics supply chain assurance. In *Emerging Topics in Hardware Security*, pages 1–26. Springer, 2020.

[181] Nidish Vashistha, Muhammad Monir Hossain, Md Rakib Shahriar, Farimah Farahmandi, Fahim Rahman, and Mark M Tehranipoor. echain: a blockchain-enabled ecosystem for electronic device authenticity verification. *IEEE Transactions on Consumer Electronics*, 68(1):23–37, 2021.

[182] Akshay Kulkarni, Noor Ahmad Hazari, and Mohammed Niamat. Ring oscillator puf and blockchain: A way of securing post fabrication fpga supply chain. In *2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 35–39. IEEE, 2023.

[183] Mark Campbell. Beyond zero trust: Trust is a vulnerability. *Computer*, 53(10):110–113, 2020.

[184] S. Mitchell & S. Connelly S. W. Rose, O. Borchert. Zero trust architecture. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Online.

[185] J. Kindervag. No more chewy centers : Introducing the zero trust model of information security. https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf. Online.

[186] Mayra Samaniego and Ralph Deters. Zero-trust hierarchical management in iot. In *2018 IEEE International Congress on Internet of Things (ICIOT)*, pages 88–95, 2018.

[187] J. Kindervag. Build security into your network's dna: The zero trust network architecture. https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. Online.

[188] S. Rose & A. Tan A. Kerman, O. Borchert. Implementing a zero trust architecture. https://csrc.nist.gov/pubs/pd/2020/10/21/implementing-a-zero-trust-architecture/final. Online.

[189] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, and Brian Lee. Access control policy enforcement for zero-trust-networking. In *2018 29th Irish Signals and Systems Conference (ISSC)*, pages 1–6. IEEE, 2018.