






Review

Review of Authentication, Blockchain, Driver ID Systems, Economic Aspects, and Communication Technologies in DWC for EVs in Smart Cities Applications

Narayanamoorthi Rajamanickam ^{1,*}, Pradeep Vishnuram ¹, Dominic Savio Abraham ¹, Miroslava Gono ², Petr Kacor ² and Tomas Mlcak ²

- ¹ Wireless Charging Research Centre, Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur 603203, India; pradeepv@srmist.edu.in (P.V.); dominica@srmist.edu.in (D.S.A.)
- ² Faculty of Electrical Engineering and Computer Science VSB-Technical University of Ostrava, 708 00 Ostrava, Czech Republic; miroslava.gono@vsb.cz (M.G.); petr.kacor@vsb.cz (P.K.); tomas.mlcak@vsb.cz (T.M.)
- * Correspondence: narayanr@srmist.edu.in

Highlights:

What are the main findings?

- Provides insights on fast, lightweight authentication and highlights how blockchain enhances security, privacy, and efficiency in IoV for DWC systems.

What is the implication of the main finding?

- Provides insights into driver identification for EV safety and comfort, and analyzes the economic viability of DWC for the EV ecosystem.



Citation: Rajamanickam, N.; Vishnuram, P.; Abraham, D.S.; Gono, M.; Kacor, P.; Mlcak, T. Review of Authentication, Blockchain, Driver ID Systems, Economic Aspects, and Communication Technologies in DWC for EVs in Smart Cities Applications. *Smart Cities* **2024**, *7*, 3121–3164. <https://doi.org/10.3390/smartcities7060122>

Academic Editor: Pierluigi Siano

Received: 28 June 2024

Revised: 15 October 2024

Accepted: 22 October 2024

Published: 24 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: The rapid advancement and adoption of electric vehicles (EVs) necessitate innovative solutions to address integration challenges in modern charging infrastructure. Dynamic wireless charging (DWC) is an innovative solution for powering electric vehicles (EVs) using multiple magnetic transmitters installed beneath the road and a receiver located on the underside of the EV. Dynamic charging offers a solution to the issue of range anxiety by allowing EVs to charge while in motion, thereby reducing the need for frequent stops. This manuscript reviews several pivotal areas critical to the future of EV DWC technology such as authentication techniques, blockchain applications, driver identification systems, economic aspects, and emerging communication technologies. Ensuring secure access to this charging infrastructure requires fast, lightweight authentication systems. Similarly, blockchain technology plays a critical role in enhancing the Internet of Vehicles (IoV) architecture by decentralizing and securing vehicular networks, thus improving privacy, security, and efficiency. Driver identification systems, crucial for EV safety and comfort, are analyzed. Additionally, the economic feasibility and impact of DWC are evaluated, providing essential insights into its potential effects on the EV ecosystem. The paper also emphasizes the need for quick and lightweight authentication systems to ensure secure access to DWC infrastructure and discusses how blockchain technology enhances the efficiency, security, and privacy of IoV networks. The importance of driver identification systems for comfort and safety is evaluated, and an economic study confirms the viability and potential benefits of DWC for the EV ecosystem.

Keywords: dynamic wireless charging; electric vehicle; authentication; blockchain; Internet of Vehicles (IoV); driver identification

1. Introduction

DWC represents a revolutionary approach to EV charging, enabling vehicles to charge on the go via power transmitters embedded in roadways [1]. This technology promises to

alleviate range anxiety—a common concern among EV users—by reducing the need for frequent stops to recharge. However, the authentication of an EV has been playing a crucial role in finding an appropriate user to charge their EV. Hence, authentication algorithms that are accurate but also efficient and fair are necessary for billing schemes to establish effective EV charging [2]. Moreover, fair billing improves EV owner's coordination in addition to enhancing their contribution to further development of DWC systems. However, the establishment of effective authentication for dynamic EV charging is not an easy task and requires multiple modules to coordinate and function [3]. In addition, when an EV comes in contact with the identity equipment, there have to be low latency communications with the help of rapid authentication protocols to guarantee that only a valid user is allowed, thereby directing the gateway to be opened. In [4], the authors mainly emphasize the billing and authentication aspects among EVs traveling over DWC lanes. In this approach, the authentication and registration with the DWC infrastructure are taken care of by the CSC. This scheme makes use of symmetric and asymmetric encryption; pseudonyms, i.e., fake names; and lightweight hashing in EV authentication with the charging segments [5,6]. The integration of vehicle networks into the Internet of Vehicles (IoVs) marks a significant advancement in enhancing performance and overcoming the limitations of intelligent transportation systems (ITS) [7]. The IoV employs two primary communication modes: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. These modes utilize control solution communications and on-board units (OBUs) to gather data, enabling real-time actions by vehicles and traffic controllers [8].

Traditional IoV architecture relies on V2V and V2I communications, but its applications remain underdeveloped and fraught with challenges [9]. Blockchain technology, a popular distributed ledger, offers a promising solution to these issues within IoVs [10]. By providing low-cost credit facilities for fundamental information management, blockchain enhances the IoV environment by ensuring transparency, immutability, and privacy. For example, blockchain can store comprehensive lifecycle information for vehicles, including certificates and insurance data [11]. Its incentive mechanisms can foster vehicle cooperation, and smart contract technology ensures secure and efficient execution processes. The IoV, a rapidly growing field, refers to a network of interconnected vehicles that communicate with each other and external systems to exchange data and offer services to drivers and passengers [12]. With the increasing complexity of IoV systems, the need for secure and efficient data exchange and storage solutions becomes more pressing. Blockchain technology, as a decentralized and distributed database, provides secure and transparent data storage and transactions, maintaining data integrity and offering tamper-proof records [13]. Recent research has extensively explored blockchain applications in IoV systems, revealing key benefits. One major advantage is secure and reliable data exchange, crucial for safety-critical applications like autonomous driving where data accuracy and integrity are paramount [14]. Several blockchain-based solutions have been proposed, such as using smart contracts to manage and enforce data access and sharing policies and employing permissioned nodes to ensure secure and efficient data exchange. Blockchain technology also enhances IoV systems by facilitating secure and transparent payment systems [15]. Traditional payment systems involve intermediaries like banks and payment processors, which increase costs and cause delays. Blockchain-based payment systems can eliminate intermediaries, enabling faster and more efficient transactions. For instance, a proposed blockchain-based payment system for EV charging allows users to pay directly at charging stations using cryptocurrency [16]. Additionally, blockchain can provide secure and transparent records of vehicle ownership and maintenance history, reducing fraud and improving the efficiency of registration and maintenance processes. For example, a blockchain-based vehicle registration system using smart contracts can automate the process and ensure secure record-keeping [17]. Overall, blockchain technology has the potential to significantly enhance the security, efficiency, and transparency of IoV systems. However, challenges such as scalability, interoperability, and regulatory issues remain. Further research is needed to develop and test blockchain-based solutions to address these

challenges and ensure secure and efficient IoV systems [18]. As electric vehicles gain prominence in urban transportation due to their rapid acceleration, strong power, energy efficiency, and reduced emissions, these advancements become increasingly vital [19].

Given the crucial role of drivers in the safety of urban public transit, driving safety is a top research priority in the field of DWC of EV technology [19]. A fundamental aspect of designing an intelligent cockpit is driver identification. By accurately recognizing the driver, the system can tailor the driving experience to enhance safety and comfort. Driver identification techniques have numerous applications, including advanced driver assistance systems, fleet management, driver profiling, vehicle anti-theft, auto insurance services, and ride-hailing platforms [20]. For instance, these techniques can call personalized program parameters for individualized driving support and reduce vehicle misuse and theft by comparing the driver's information with authorization data. They can also automatically adjust seat alignment and air temperature based on the driver's preferences. In ride-hailing services, driver identification can improve service quality, especially with shared vehicles [21]. In the context of intelligently networked vehicles and traffic control systems, driver identification has significant market potential and research relevance, becoming a hot topic in recent years [22]. Research in engineering management and intelligent transportation has yielded significant advances in driver identification. The main objectives are to quickly and accurately determine driver identity and to create personalized operations for enhanced driving and traffic safety. Researchers have developed driver recognition methods with varying levels of granularity based on specific requirements [23]. The core workflow of driver identification involves four steps: data collection, data processing, driver identification, and result application. The process begins with collecting a variety of driving-related data, such as driving behavior, vehicle movement, and road conditions [24]. This data must be preprocessed—through extraction, segmentation, or normalization—to ensure high quality and proper arrangement. Concurrently, data features should be designed and selected. The third stage involves identifying the driver. Various techniques are used to fuse the collected data and create a model linking data characteristics to drivers, which is then used for identification [25]. Finally, the outcomes of driver identification are applied in engineering applications like personalized driving assistance and auto insurance. Early research employed techniques such as hidden Markov models (HMM) [26], Gaussian mixture models (GMM) [27], random forest (RF) [28], support vector machines (SVM) [29], linear discriminant analysis (LDA) [30], artificial neural networks (ANN) [31], K-nearest neighbors (KNN) [32], and extremely randomized trees (ET) [33].

Several studies have analyzed the economic implications of dynamic charging. A study by the IEA in 2020 found that dynamic charging could reduce the need for a public charging infrastructure, thereby reducing costs for governments and taxpayers [34,35]. The study also found that dynamic charging could improve the utilization of the charging infrastructure, leading to a more efficient charging network. Another study by the NREL in 2019 analyzed the economic viability of dynamic charging for electric buses [36]. The study found that dynamic charging could reduce battery size and cost, leading to significant savings for fleet operators. The study also found that dynamic charging could enable the electrification of bus routes that were previously considered impractical due to range limitations.

A 2021 study by the European Commission analyzed the cost-effectiveness of dynamic charging compared to static charging for electric buses [37]. The study found that dynamic charging could be more cost-effective in certain scenarios, particularly for high-capacity buses that require larger batteries. Hence, the need for a DWC system is crucial for smart cities applications with suitable authentication, blockchain technology for data communication, and driver identification approaches [38]. This paper provides a comprehensive survey of the above-mentioned topics for the DWC of EV. Figure 1 shows the section-wise structure of this review paper. The major contributions of this review paper are as follows:

- The manuscript explores the integration of DWC technology for EV, particularly focusing on critical components like authentication techniques, blockchain applications, driver identification systems, and communication technologies.
- The study emphasizes the importance of fast and lightweight authentication systems for secure access to the DWC infrastructure, along with blockchain's role in decentralizing and securing vehicular networks to improve privacy and efficiency within the IoV architecture.
- The economic aspects of implementing DWC are thoroughly evaluated, offering insights into its feasibility, cost implications, and potential impact on the broader EV ecosystem.
- By providing a comprehensive analysis of current technologies and challenges, the manuscript offers valuable guidance for advancing the DWC infrastructure and integrating it into smart city applications.

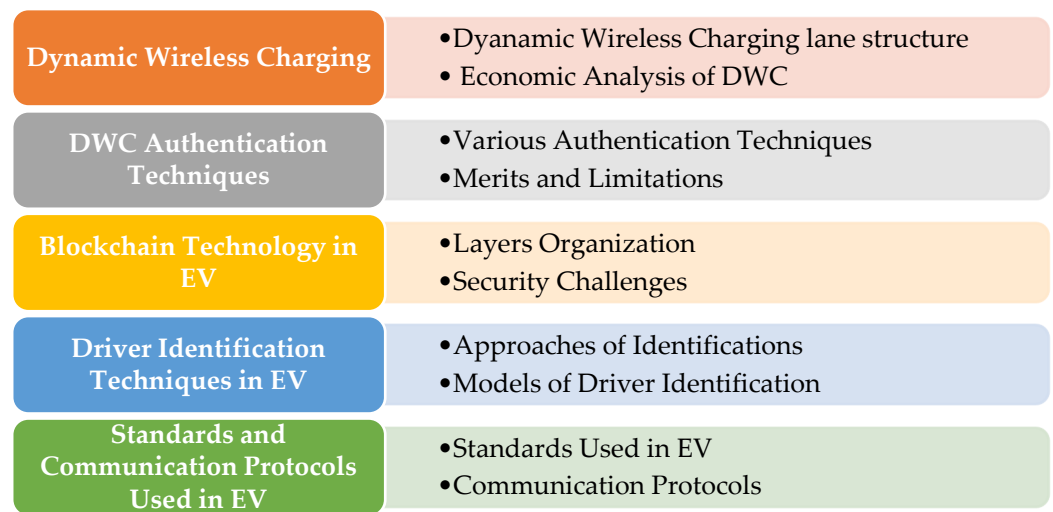


Figure 1. Sectional-wise structure of the manuscript.

The remainder of this paper is organized as follows: Section 2 provides a description of DWC construction and its economic analysis, and Section 3 presents different types of authentication techniques used in the DWC system. Section 4 then outlines the related works on blockchain and its applications in IoVs. The driver identification system and various models are presented in Section 5. Standards and protocols and new communication technologies for EVs are presented in Sections 6 and 7, which concludes the paper.

2. Dynamic Charging Technology

Dynamic charging refers to the method of wirelessly charging EVs while they are in motion. This technology involves embedding wireless charging technology in the road, allowing EVs to charge their batteries as they drive. Dynamic charging has the potential to significantly minimize range anxiety for EV drivers, as they would no longer need to stop and charge their vehicles at designated charging stations [39]. It could also reduce the need for large battery sizes in EVs, as they could charge more frequently while on the road. However, the implementation of dynamic charging technology would require significant infrastructure investments, including the installation of wireless charging technology in roadways and the upgrading of the electricity grid to handle the increased demand for power [40]. Additionally, there are potential safety concerns related to the use of dynamic charging technology, as well as the impact on traffic flow and the need for regulatory and standardization frameworks. Overall, while dynamic charging has the potential to revolutionize EV charging, there are significant technological, economic, and regulatory challenges to be overcome before it is widely accepted.

2.1. DWC System and Charging Demand Estimation of EVs

Estimating the charging demand of EVs using wireless charging technology would involve analyzing factors such as the count of EVs on the lane, the driving patterns of EV users, the charging capacity of the wireless charging infrastructure, and the availability and accessibility of the charging infrastructure. One approach to estimating charging demand is to use data from existing EVs and their charging behaviors [41]. These data can be used to estimate the average distance driven per day, the average time spent driving, and the average charging requirements of EVs. This information can then be used to estimate the number of charging stations and the capacity of the wireless charging set-up needed to meet the demand. Another approach is to use simulation models to estimate charging demand. These models can take into account factors such as EV adoption rates, the availability of the wireless charging infrastructure, and the impact of various policies and incentives on EV charging behavior [42]. Overall, accurately estimating the charging demand of EVs using wireless charging technology would require a comprehensive understanding of the various factors that influence EV charging behavior and the development of appropriate modelling tools and data sources to estimate charging demand. Elongated tracks (more than 10 m) serve as transmitter pads in a DWPT framework in Figure 2a to charge EVs while they are moving [43]. Another DWPT construction with numerous lumped pads inserted in the pavement is shown in Figure 2b [44]. In order to combine the advantages (and disadvantages) of the two previously mentioned layouts, elongated pads, which are depicted in Figure 2c, are broader than combined pads but shorter compared to long rails.

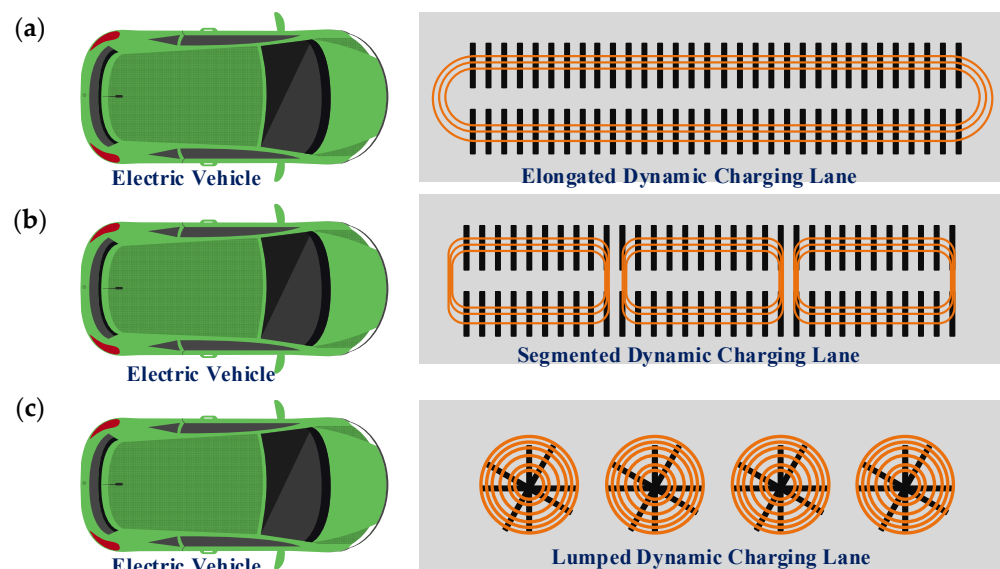


Figure 2. DWC system: (a) Elongated rails; (b) Lumped pads; (c) Elongated pads.

The DWC technique has successfully satisfies the needs of electric car charging times and area while reducing the size of the vehicle rechargeable battery, extending the cruise range, and using only existing road resources [45]. It should be mentioned that when driving on non-charging roads, a specific quantity of battery is required for cars to maintain a specific distance. The transmitting side and receiving side make up the majority of a DWC for electric cars. Transmitting coils, compensation networks, and high-frequency inverters are the major components of the transmitting side. The primary components of the receiving side include battery packs, AC-DC rectifier filters, compensation networks, and receiving coils. The transmitting coils in the dynamic charging system locate the receiver coil and then turn on the transmitting coils next to it [46]. The transmission coils are disabled if there are no cars to save electricity. Figure 3a shows the schematic view of DWC, and Figure 3b illustrates the view of the expressway from the top.

2.2. Structure of Dynamic Wireless Charging

The building cost of DWC is determined by several factors, such as the kind of technology used, the magnitude of the charging infrastructure, and the location of the charging system. One of the main components of a DWC system is the charging pads, which are installed on the road or in designated charging areas [47]. The cost of the charging pads will depend on the type of technology used, such as inductive or resonant charging, and the size and capacity of the pads. Typically, larger and higher-capacity pads will be more expensive than smaller and lower-capacity pads [48]. Another component of a DWC system is the power electronics and control systems, which are used to manage the flow of electricity between the charging pads and the vehicles. The cost of these systems will depend on their complexity and capacity, as well as the level of automation and control needed [49]. In addition to the charging pads and control systems, the construction cost of DWC will also include the cost of installation, including excavation and trenching for the charging infrastructure, as well as the cost of any necessary modifications to the road or charging areas.

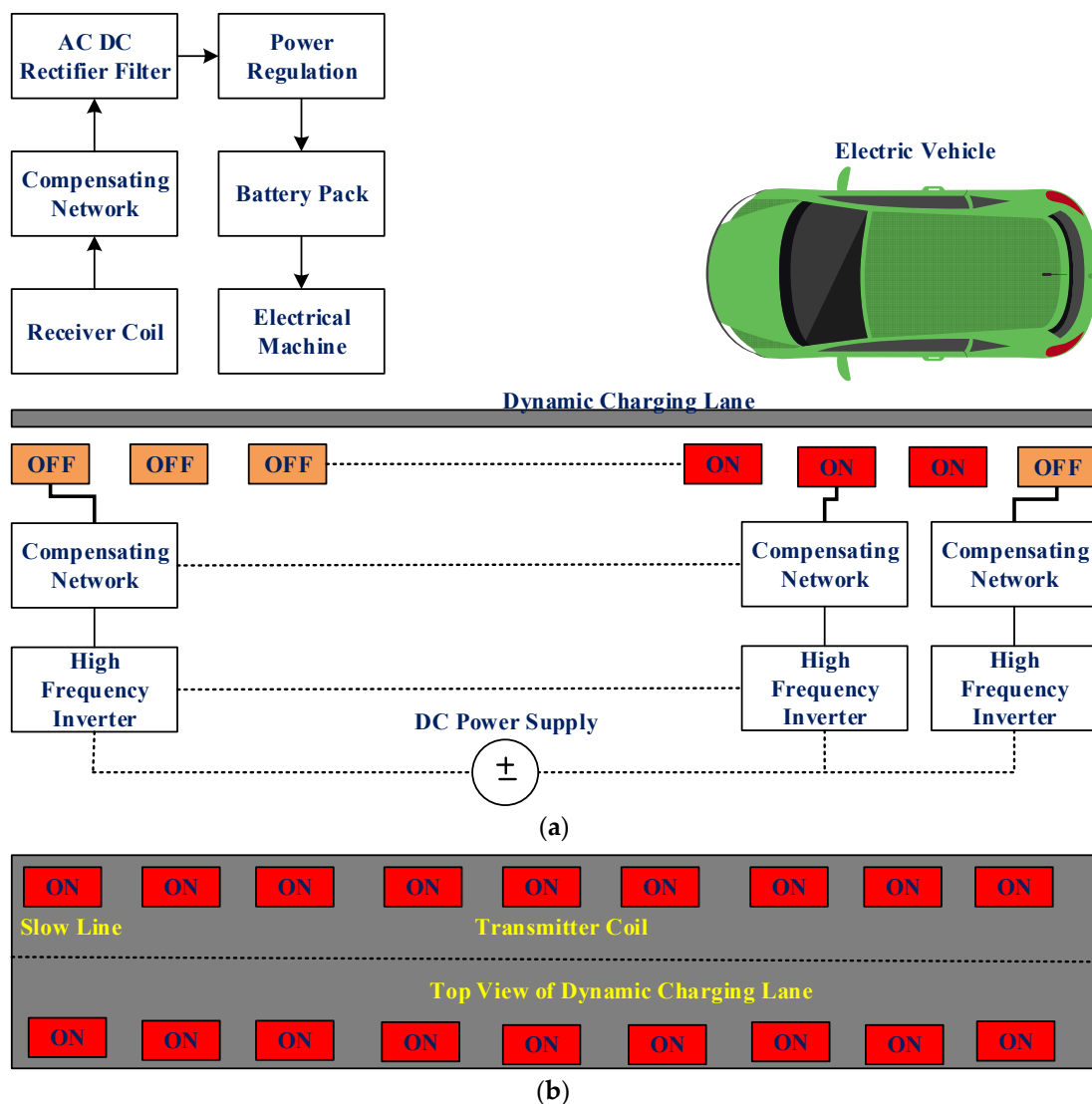


Figure 3. (a) DWC schematic; (b) Top view expressway.

The location of the charging system can also impact the construction cost. For example, if the charging infrastructure is installed in a highly populated or urban area, there may be additional costs associated with traffic management and permits. Overall, the construc-

tion cost of dynamic wireless charging can vary widely depending on these and other factors [50]. However, it is generally expected to be beyond the cost of a static charging infrastructure because of the additional complexity and technology required.

2.3. Types of Economic Analysis of DWC System

There are several types of economic analysis that can be used to assess the viability and benefits of dynamic charging technology. The following are some of the most common types:

- Cost-Benefit Analysis (CBA)

This kind of economic analysis compares the costs and benefits of a project or investment to determine its overall economic viability [51]. In the context of dynamic charging, a CBA would compare the costs of building and operating the infrastructure with the benefits of reduced emissions and increased convenience for electric vehicle owners. The analysis would need to consider both the direct costs, such as the cost of building and operating the charging infrastructure, as well as the indirect costs, such as the opportunity cost of using resources for this project instead of other projects.

- Life-Cycle Cost Analysis (LCCA)

LCCA is a type of economic analysis that considers all budgets related with a scheme over its whole life cycle [51]. In the context of dynamic charging, an LCCA would consider the expenses of building as well as operating the charging set-up, as well as the cost of disposing of the equipment at the termination of its valuable life. This analysis may allow decision-makers to compare the long-term costs of dynamic charging with alternative solutions.

- Net Present Value (NPV) Analysis

This kind of economic study contrasts the present value of expected cash flows with the current value of expected cash outflows using a reduced cash flow analysis [51]. An NPV analysis would take into account the initial investment in developing the charge stations, as well as the continuing operational expenses and income for charging electric vehicles. The analysis would calculate the investment's net present value while accounting for the net present value.

- Return on Investment (ROI) Analysis

ROI is a type of economic study that compares the return on an investment with the cost of the investment [51]. In the context of dynamic charging, an ROI analysis would compare the revenue generated by the charging infrastructure with the initial investment in building the infrastructure. The analysis would provide decision-makers with an estimate of the financial return on the investment in dynamic charging technology.

- Sensitivity Analysis

Sensitivity analysis is a kind of commercial analysis that explores the impact of changes in assumptions on the results of the analysis [51]. In the context of dynamic charging, a sensitivity analysis would explore the impact of changes in factors such as electricity prices, vehicle adoption rates, and infrastructure costs on the viability of the technology. This analysis would help decision-makers to identify the key assumptions driving the analysis and assess the robustness of the results.

There are several equations used in the economic analysis of dynamic charging. Some of the key equations include the following:

- Total Cost of Ownership Equation

This equation is used to calculate the total cost of owning an electric vehicle, taking into account the initial purchase cost, operating costs (such as electricity and maintenance), and the residual value of the vehicle [52].

$$TCO = Purchase_cost + Operating_costs - Residual\ value \quad (1)$$

Assuming a typical electric vehicle with a range of 100 miles, a battery capacity of 60 kWh, and an electricity cost of \$0.12 per kWh, the TCO of the vehicle over 5 years can be calculated as follows:

Purchase cost = \$35,000

Operating costs = $(\$0.12/\text{kWh} \times 60 \text{ kWh} \times 100 \text{ miles}/100 \text{ miles}) \times 5 \text{ years} = \4320

Residual value = \$15,000

TCO = $\$35,000 + \$4320 - \$15,000 = \$24,320$.

- Levelized Cost of Electricity Equation

This equation is used to calculate the average cost of electricity over the lifetime of a dynamic charging system. It takes into account the initial capital cost, operating costs, and the amount of electricity generated [52]. Assuming a dynamic charging system with a capital cost of \$1 million, an operating cost of \$50,000 per year, and an electricity generation capacity of 500 MWh over 10 years, the LCOE of the system can be calculated as follows:

Total cost = \$1 million + $(\$50,000 \times 10 \text{ years}) = \1.5 million

$$LCOE = \$1.5 \text{ million} / (500,000 \text{ kWh} \times 10 \text{ years}) = \$0.03/\text{kWh} \quad (2)$$

- Net Present Value (NPV) Equation

The net present value equation is employed to determine the current value of upcoming cash flows while accounting for time value of money. It is frequently used to evaluate an investment's profitability [52].

$$NPV = \sum \left(\frac{CF_t}{(1+r)^t} \right) \quad (3)$$

where CF_t is the cash flow in year t , r = discount rate, t = year. Assuming an investment of \$1 million in a dynamic charging system with expected cash flows of \$200,000 per year over 10 years, a discount rate of 8%, and a residual value of \$100,000, the NPV of the investment can be calculated as follows:

$$NPV = \$422,170 \quad (4)$$

- Internal Rate of Return (IRR) Equation

This equation is used to figure out how much a return on investment will be. It is the valuation method at which an investment has no net present value [52].

$$NPV = \sum \left(\frac{CF_t}{(1+IRR)^t} \right) \quad (5)$$

where CF_t = cash flow in year t , t = year, IRR = internal rate of return. Using similar investment assumptions to those above, the IRR of the investment can be computed by finding the concession rate that creates the NPV of the investment identical to zero:

$$IRR = 12.2\% \quad (6)$$

- Benefit-Cost Ratio (BCR) Equation

The benefit-cost ratio equation is used to assess the economic viability of an investment. It is the proportion of the present value of benefits to the present value of costs [52].

$$BCR = \sum \left(\frac{B_t}{(1+r)^t} \right) / \sum \left(\frac{C_t}{(1+r)^t} \right) \quad (7)$$

where B_t = benefits in year t , C_t = costs in year t , r = concession rate, t = year. Assuming a dynamic charging system with a benefit of \$300,000 per year and a cost of \$100,000 per year, over a 10-year period, the BCR of the investment can be calculated as follows:

$$\begin{aligned} \text{Benefits} &= \$300,000 \times 10 \text{ years} = \$3 \text{ million} \\ \text{Costs} &= \$100,000 \times 10 \text{ years} = \$1 \text{ million} \\ \text{BCR} &= \$3 \text{ million} / \$1 \text{ million} = 3 \end{aligned}$$

These equations can be used to assess the economic viability of dynamic charging in different contexts, such as for electric buses or personal electric vehicles. By using these equations, it is possible to determine the potential cost savings and benefits of adopting dynamic charging technology and to compare it to other charging solutions. Calculations for the economic analysis of dynamic charging depend on several factors, including the specific context of the analysis, such as the type of electric vehicle or the location of the charging infrastructure. However, the following is an example of calculations that can be used to assess the economic likelihood of dynamic charging. To calculate the costs and benefits, we used data from a pilot project in Sweden, which involved the setting up of a dynamic charging set-up on a 2 km stretch of road. The direct costs of the project were estimated to be €1.6 million, with ongoing operating costs of €27,000 per year. The indirect costs were estimated to be €1.1 million, based on the opportunity cost of using resources for this project instead of other projects [53].

The benefits of the project were estimated to be a reduction in CO₂ emissions of 138 tons per year, based on the assumption that 100 EVs would use the dynamic charging infrastructure daily. The increased convenience for EV owners was estimated to result in a 10% increase in EV adoption in the region. The potential economic benefits were estimated to be €1.2 million per year, based on the assumption that increased EV adoption would result in increased demand for EVs, driving innovation and job creation in the EV industry. Based on these estimates, the NPV of the project was calculated to be €2.2 million, with a BCR of 1.9. These example calculations illustrate how economic analysis can be used to assess the viability of dynamic charging technology and the potential cost savings and benefits of adopting it. The specific calculations will depend on the context and assumptions used in the analysis.

2.4. Challenges

Economic analysis of dynamic charging can be challenging due to various factors. Some of the challenges are as follows:

- Complexity of the technology

Dynamic charging involves a complex system of infrastructure, vehicles, and power grids. Economic analysis of dynamic charging requires a detailed understanding of this system, which can be challenging.

- Interdisciplinary nature

Economic analysis of dynamic charging requires expertise in economics, engineering, and other fields. This interdisciplinary nature can make it challenging to find individuals or teams with the necessary skills to conduct an effective analysis.

- Limited data availability

As mentioned earlier, economic analysis requires data on variables such as consumer behavior and infrastructure costs. However, there may be limited data available on these variables, which can limit the accuracy of the analysis.

- Difficulty in estimating costs and benefits

Economic analysis of dynamic charging involves estimating the costs and benefits of the technology, which can be challenging due to the uncertainty of future developments, such as battery costs and performance.

- Heterogeneous adoption

The adoption of dynamic charging may be heterogeneous across different regions, vehicles, and driving patterns. This heterogeneity can make it challenging to conduct an

analysis that accurately captures the costs and benefits of dynamic charging for different groups of people and regions.

- Time lag

Economic analysis is often conducted retrospectively, after the technology has been implemented. However, the time lag between implementation and analysis can mean that the analysis is not timely, and the findings may not be as relevant as they could be.

In summary, economic analysis of dynamic charging can be challenging due to the complexity of the technology, the interdisciplinary nature of the analysis, limited data availability, difficulty in estimating costs and benefits, heterogeneous adoption, and the time lag between implementation and analysis. Despite these challenges, commercial analysis can still provide rich insights into the benefits and costs of dynamic charging.

2.5. Advantage of Economic Analysis of Dynamic Charging

Dynamic charging, which refers to the ability to charge EVs on the move, has been identified as a potential solution to the problem of range concern, which is a major obstruction to the acceptance of EVs. Economic analysis of dynamic charging can provide valuable insights into the costs and benefits of this technology. Some of the advantages of economic analysis of dynamic charging are as follows:

- Identifying cost savings: Economic analysis can help identify cost savings associated with dynamic charging, such as reduced battery size, which can result in a lower cost of ownership for EVs.
- Assessing the economic feasibility: Economic analysis can assess the economic possibility of DC by determining costs of implementing the infrastructure and the potential revenue streams that can be generated from the technology. This can help policymakers and investors determine whether dynamic charging is a worthwhile investment.
- Evaluating the influence on the power grid: Dynamic charging can have a significant influence on the power grid, as it requires a large amount of electricity to be supplied to the charging infrastructure. Economic analysis can evaluate the influence of dynamic charging on the power grid and determine the infrastructure requirements necessary to support the technology.
- Understanding the impact on consumer behavior: Economic analysis can help understand the impact of dynamic charging on consumer behavior, such as the willingness to pay for dynamic charging services and the potential increase in demand for EVs.
- Supporting policy development: Economic analysis can support the development of policies and regulations related to dynamic charging by providing insights into the costs and benefits of technology on the environment and society.

Overall, commercial analysis can offer rich insights into the benefits and costs of dynamic charging, which can help policymakers, investors, and consumers make informed decisions about the adoption of this technology.

2.6. Limitations in Economic Analysis of Dynamic Charging

While commercial analysis can provide rich insights into the benefits and costs of dynamic charging, there are also some limitations to this approach. Some of the limitations include the following:

- Uncertainty about future technology: Economic analysis relies on assumptions about future technology, such as the cost and performance of batteries and charging infrastructure. These assumptions can be uncertain, and if the technology does not develop as expected, the economic analysis may be inaccurate.
- Lack of data: Economic analysis requires data on variables such as consumer behavior and infrastructure costs. However, data on these variables may be limited or difficult to obtain, which can limit the accuracy of the analysis.
- Difficulty in accounting for externalities: Economic analysis typically focuses on the private costs and benefits of dynamic charging, such as the cost of infrastructure

and the savings from reduced battery size. However, dynamic charging can also have externalities, such as reduced air pollution, that are difficult to account for in economic analysis.

- Limited scope: Economic analysis is typically focused on specific outcomes, such as the cost-effectiveness of dynamic charging. However, there may be broader social, environmental, and equity considerations that are not fully captured in economic analysis.
- Geographical and temporal limitations: Economic analysis may not be generalizable to different geographical contexts or time periods. For example, the costs and benefits of dynamic charging may vary depending on the region or country, and economic analysis may not capture the long-term impacts of the technology.

Overall, while economic analysis delivers valuable visions of the costs and benefits of dynamic charging, it is vital to know its limitations and to complement economic analysis with other types of analysis, such as environmental and social impact assessments.

3. Authentication Techniques

There are various authentication techniques described in the literature, but here only prominent techniques used in DWC of EVs are discussed:

- Symmetric and Asymmetric Cryptography

Public-key cryptography or asymmetric cryptography is one of the techniques used for authentication, where keys are in pairs, such as private and public keys, for coding and decoding [54]. With the help of the receiver's public key, a message can be encrypted in public-key cryptography, and only the particular receiver with the use of a private key can decrypt the message [55]. Nevertheless, a shared key is employed for both coding and decoding in symmetric-key cryptography. Figure 4 explains the complete procedure of symmetric encryption.

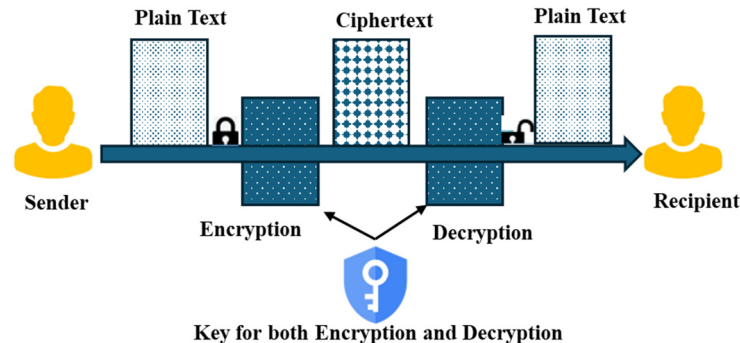


Figure 4. Process of symmetric encryption.

Four cryptographic goals mostly detect and prevent fake users from stealing, altering, tampering with, etc., the specific data. These goals are classified as follows:

- Confidentiality

It is a methodology to ensure that data can be accessed only by authorized persons. To obscure data and provide confidentiality, numerous techniques can be used, such as physical protection and encryption procedures [56].

- Data integrity

In this process, it must be ensured that the data is sent completely and without any modifications. Data modifications can occur through substitution, insertion, and deletion [57].

- Authentication

In the process, the recipient has to identify whether the captured data has come directly from the authorized sender or not [58].

- Non-repudiation

In this process, both senders, as well as recipients, are ensured not to refuse the transmission, which means that the sender should not deny transmitting the data, and similarly, the recipient should not deny capturing the data sent by the sender [58].

- Digital signatures

It is one type of cryptographic procedure that checks the faithfulness of a message or a digital file. To transmit information across an unclear channel, asymmetric cryptography uses this protocol. Here, the end user can authenticate whether or not the note or message is sent by the authorized dispatcher [59]. The mostly used digital signature protocols or techniques are DSA, RSA, and ECDSA [60,61]. Of all of these, ECDSA is the highly suggested digital signature structure, and it is considered the IEEE 1609.2 standard [62,63]. Signature verification, key generation, and algorithm signing are the three steps incorporated into digital signature schemes.

- Hash chains

A hash function remains a mathematical one-way function, where a message is mapped from a random size to a static-sized message, which can be utilized for effective verification. In general, a hash chain is considered a chain of numerous one-way hash functions obtained by means of hash algorithms like SHA-1 or SHA-2 [64]. The primary key is chosen uncertainly, and the left-out keys are mathematically estimated with the help of the H. An individual key can be initiated by $K_j = H(K_{j-1})$ for $j = 1, 2, 3, \dots, n$ [65]. Figure 5 shows the sample four-key hash chain.

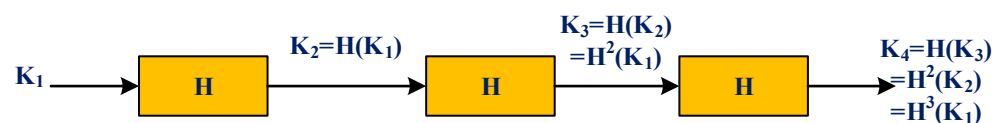


Figure 5. Sample four-key hash chain.

- Fast Authentication for Dynamic EV Charging

Fast message signing, quick signature verification, quick handoff authentication, and little communication overhead are all aspects of FADEC proposed in [66]. To avoid having to re-authenticate each time an RSU is encountered without compromising security, FADEC enables the electric vehicle to utilize the identical key to verify with a number of RSUs. FADEC enhances the delivery ratio by greater than an order of magnitude and cuts the data transfer latency by up to 97% when compared to ECDSA [67]. To the extent that we are aware, this is the initial study to take secure V2G interaction for dynamic EV charging into consideration.

- Hash-based Message Authentication Code

HMAC is an authentication protocol that depends on a symmetric key, K , transferred between the receiver and the sender. Whenever the sender wishes to transmit a message M , then he uses the shared key K to compute a hash value $\text{HMAC}(K, M)$. M and $\text{HMAC}(K, M)$ are both transmitted to the recipient. By recalculating $\text{HMAC}(K, M')$ and confirming that $\text{HMAC}(K, M') = \text{HMAC}(K, M)$ after obtaining message M' as well as its signature $\text{HMAC}(K, M)$, the end user may confirm that $M' = M$ and the information is from the genuine sender (K, M). When using the right keys and hash algorithms, HMAC authentication may achieve 112-bit security level while being faster than public key-based authentication [68].

- Elliptic Curve Digital Signature Algorithm

Each interaction party in the DSA has a private key S and a public key P . The private key must only be accessible to the owner, whereas everybody is given access to the public key. The sender creates a signature $S(M)$ for the message M by signing it with his encryption key S and sending it along with the message M . When obtaining $M', S(M)$, the recipient

might compute $P(S(M))$ by using the demonstrated sender’s public key P and confirm that $M' = P(S(M))$ in order to determine the message’s authenticity. A DSA that uses elliptic curve cryptography is called an ECDSA. ECDSA is recommended by the IEEE 802.11p standard [68] as a means of authenticating vehicle safety notifications. However, prior research [69] has demonstrated that ECDSA requires non-trivial time to register or sign as well as to evaluate an autograph and is unsuitable in situations where there are numerous signatures to validate, which is typical in situations where several electric vehicles provide regular updates. The susceptibility of ECDSA to DoS threats, where the intruder might overwhelm the network with numerous bogus signatures while the receiver RSU is occupied validating those phony signatures, is another significant flaw in the protocol.

- Just Fast Keying

JFK [70] is considered as a key swap-over mechanism that is centered on Diffie-Hellman. JFK aims to make it possible for two collaborating negotiators to create a transferred undisclosed key, though the interaction medium is unsecure, meaning that the enemy might listen in on the stream. Digital signatures are used on JFK communications to guard against man-in-the-middle attacks. In addition, the main benefit of JFK is that it resists DoS attacks and shields the RSU against signature flooding attacks, in which the attacker floods the RSU with many signatures to check before it has time to verify those from trustworthy cars.

- Fast and Lightweight Privacy-Aware Authentication

FLPA has the following desirable qualities as represented in Figure 6: (1) EV users’ identity and position are kept private by unknown EV verification to the CSP and the charging setup utilizing demonstrable aliases rather than their true identities. (2) It has quick and easy authentication between EVs and charging stations that does not use the CSP and simply calls for one message passing and straightforward hash chain verification. (3) The FLPA enables fair billing and stops dishonest EVs from twice spending identical charging coins. (4) It also provides conditional anonymity, which allows only a TA to track an EV’s history for the reasons of revocation and other protective measures [71].

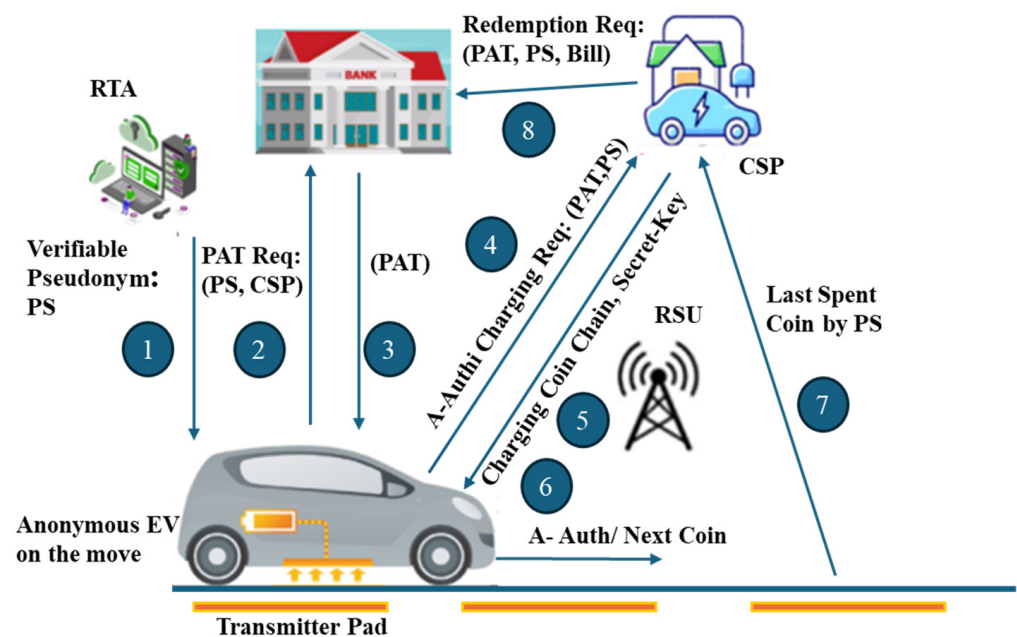


Figure 6. Architecture model of FLPA (A-Auth: anonymous authentication, PAT: payment authorization token, RTA: registration trusted authority).

4. Blockchain Technology in DWC-EV

4.1. Layers of Blockchain

The implementation of blockchain in the IoV requires a layered approach to address the complexity and security requirements of the system. Generally, the layers can be separated into three main categories: the sensing layer, the communication layer, and the application layer [72].

- Sensing Layer

This is the bottom layer of the IoV blockchain architecture, which deals with data acquisition and communication. In this layer, sensors, cameras, and other data acquisition devices gather information from the surrounding environment and transfer it to the network layer. The data gathered in this layer are highly sensitive and require secure and efficient transmission.

- Communication Layer

This layer is accountable for ensuring secure communication between diverse IoV devices and components. It is the middleware that facilitates the communication between the sensing layer as well as the application layer. The network layer delivers a secure and reliable communication channel using blockchain technology, ensuring data integrity and confidentiality.

- Application Layer

The top layer of the IoV blockchain architecture is the application layer. It involves the design and development of applications that leverage the data collected from the perception layer to provide various services to drivers and passengers. In this layer, smart contracts are deployed to automate transactions and enforce data sharing policies. The application layer includes various applications such as autonomous driving, traffic management, and smart parking.

Each layer of the IoV blockchain architecture has its own set of challenges and requirements [72]. For example, in the sensing layer, the challenge is to ensure accurate and reliable data acquisition and transmission. In the communication layer, the challenge is to design a secure and efficient communication protocol that can handle the massive amounts of data generated in the sensing layer [73]. In the application layer, the challenge is to design and develop applications that can leverage the data collected from the perception layer to provide value-added services to users. In summary, the use of blockchain technology in the IoV requires a layered approach to address the complex security and efficiency requirements of the system [74]. The sensing layer deals with data acquisition and communication, the communication layer provides a secure and reliable communication channel, and the application layer provides various services to drivers and passengers [75]. An architecture is suggested for multiple technologies in the IoV system. It is primarily comprised of five layers. An illustration of a combined blockchain and IoV design is shown in Figure 7.

Layer 1: All of the vehicle sensors make up the sensing layer, which gathers data and identifies specific events that are relevant such vehicle circumstances, driving patterns, weather conditions, etc.

Layer 2: Different wireless communication modes are made possible by the second layer that is the communication layer (e.g., V2I and V2V). Current and upcoming networks, including Wi-Fi, GSM, Bluetooth, and LTE, are often connected thanks to a communication layer.

Layer 3: A gateway between the communication layer and application levels, the blockchain serves as a governance layer. This may offer blockchain built keys and group information into blocks in such a broadened IoV architecture. Furthermore, by offering a set number of tokens in exchange for sharing information resources, it may use incentive mechanisms to encourage users to do so. This would enable users to actively contribute transactional data to the system.

Layer 4: The IoV network's third layer, or computing, is responsible for storing, analyzing, and making choices pertaining to a variety of situations. Additionally, this layer offers data computing services.

Layer 5: The IoV's topmost level, the application layer, can provide customers with a variety of various vehicle services.

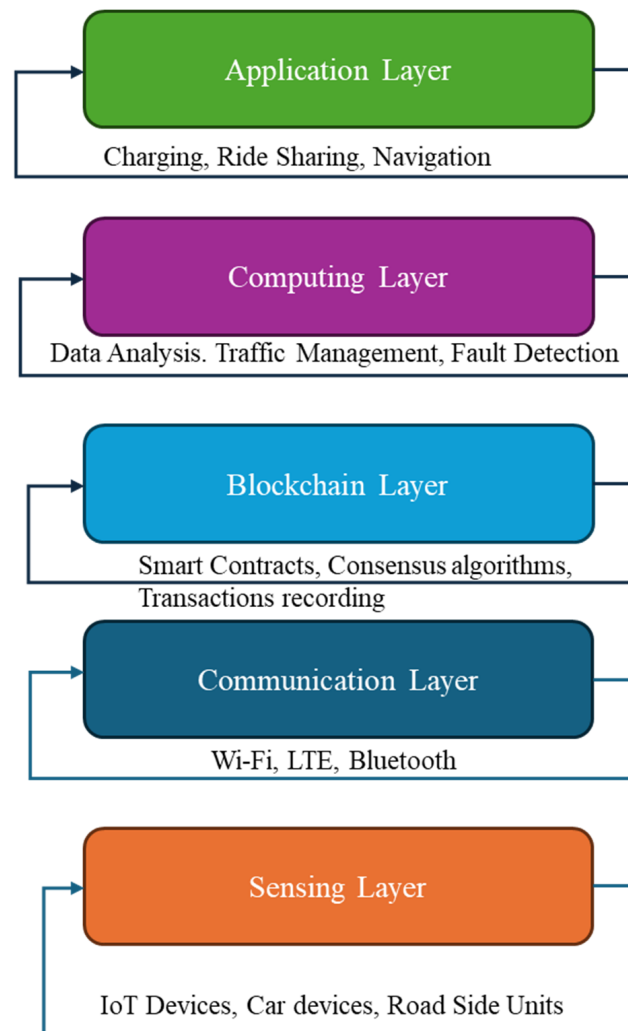


Figure 7. Blockchain and IoV architecture.

4.2. Blockchain Applications in IoV

According to their function and area of activity, blockchain applications inside the IoV were divided during the analysis process into eight major categories as shown in Figure 8: privacy and security, P2P energy trading, data safeguard and management, microgrid management, AI/ML and IoV, IoV management, block chain performance in the IoV, and general-purpose studies (e.g., reviews, surveys, etc.).

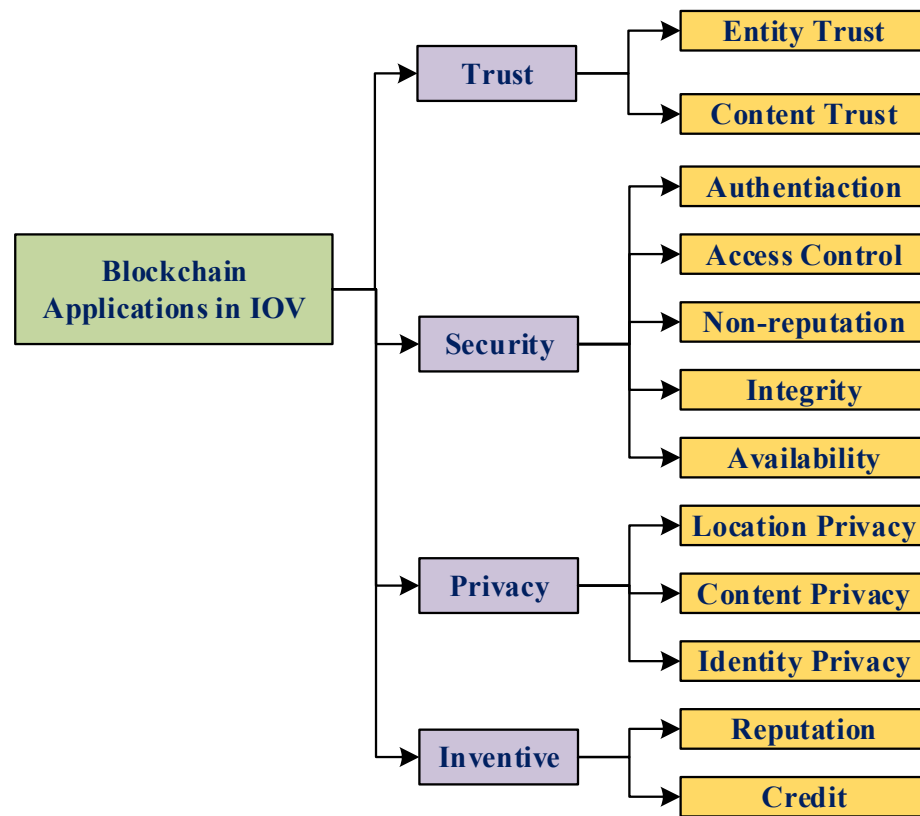


Figure 8. Applications of blockchain in IoV.

The writers discovered that about one out of three applications dealt with security and privacy (27%), including efforts for identity management, V2X, and authentication. IoV management (25.8%) was the second-most common group. P2P energy trading and general-purpose studies came in third and fourth, making up 12.7% and 12.3% of all studies, respectively. Figure 9 shows that other application fields accounted for about 22% of the total. Figure 10 shows the classification of the selected application categories.

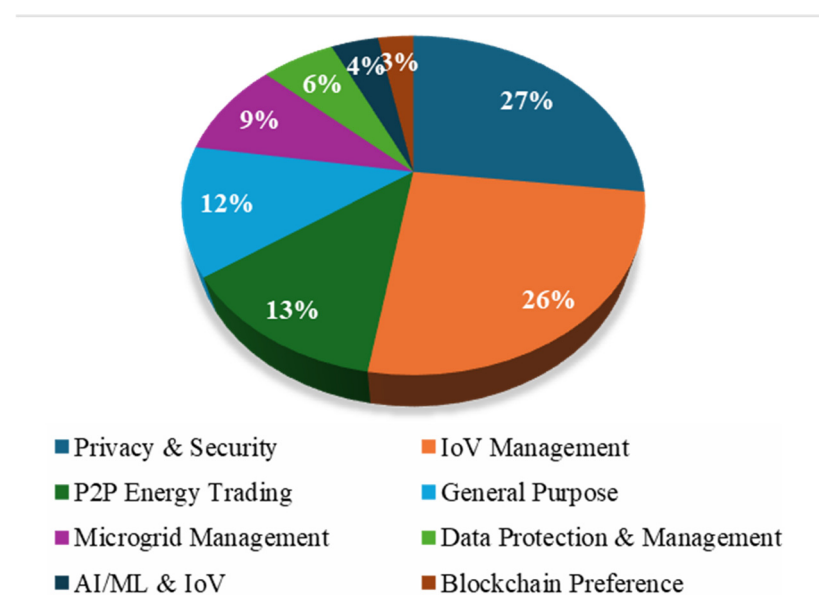


Figure 9. Blockchain applications in IoV—grouping according to their areas of application.

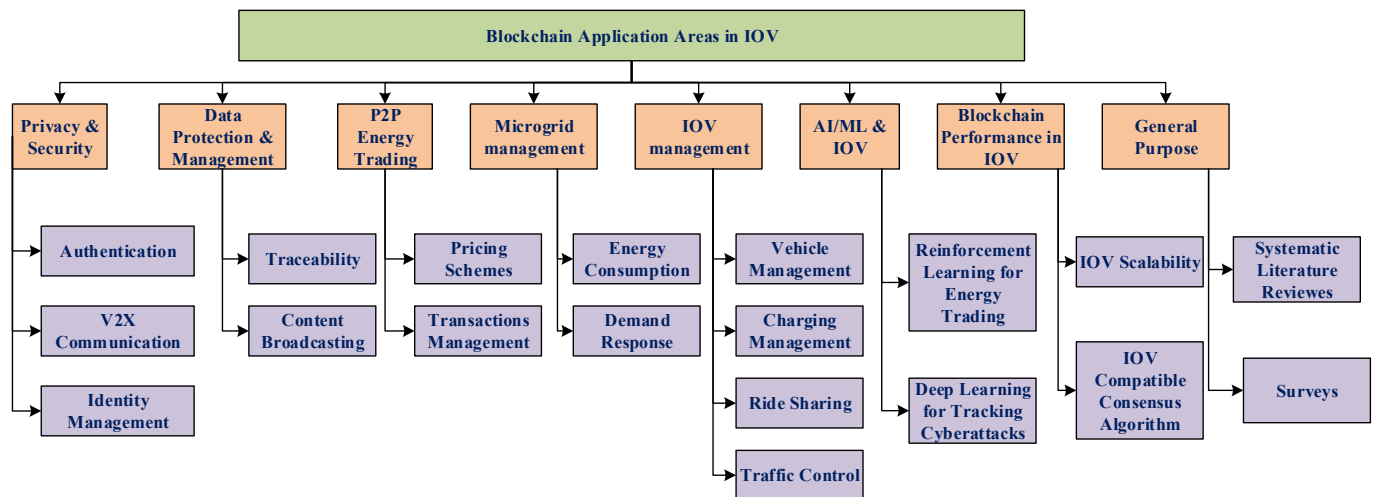


Figure 10. Blockchain application areas in the IoV.

4.3. Challenges of IoV-Assisted Smart Grid

While blockchain technology offers many potential benefits for IoV-assisted smart grids, there are also several challenges that must be addressed to fully realize its potential [76]. Here are some of the key challenges of using blockchain in IoV-assisted smart grids:

- Scalability

This is considered one of the main issues with blockchain technology, as the current blockchain technology can only manage a restricted number of transactions per second. The quantity of transactions in a large-scale grid network can soon overload the blockchain network, resulting in long transaction times and expensive fees. New scaling methods, such as sharding and layer-2 protocols, are being created to overcome this problem [77].

- Interoperability

The IoV ecosystem involves a wide variety of devices, systems, and stakeholders, each with their own data formats and communication protocols [78]. Ensuring interoperability between different blockchain-based solutions and legacy systems can be a significant challenge.

- Energy Consumption

The process of validating and adding transactions to a blockchain needs a significant quantity of computational power, leading to high energy consumption [79,80]. In a smart grid network that relies on energy-efficient solutions, this can be a significant challenge.

- Regulation and Governance

Blockchain technology until today has been in its initial stages, and there are currently few regulations governing its use. This can lead to uncertainty and confusion around the legal and regulatory frameworks for blockchain-based smart grid solutions.

- Security and Privacy

Although blockchain technology is usually regarded as safe, assaults are still possible. In addition, the use of blockchain for data storage and sharing can raise concerns around data privacy and confidentiality [81,82].

- Cost

Implementing blockchain technology in a smart grid network can be expensive, as it requires significant investment in hardware, software, and infrastructure. Additionally, the costs of transaction fees and energy consumption can add to the overall cost of the system. In summary, while blockchain technology has the possibility to transform the way we manage and distribute energy in smart grid networks, it also faces several challenges. These challenges include scalability, interoperability, energy consumption, regulation and

governance, security and privacy, and cost. Addressing these challenges will be critical to realizing the full potential of blockchain-based IoV-assisted smart grids.

- **Blockchain-based IoV Security**

Blockchain technology has the possibility to enhance the safekeeping of IoV by providing a safe and decentralized stage for storing and verifying transaction data. Here are some of the ways in which blockchain can improve the security of IoV:

- **Identity management**

Blockchain technology can be used to create a secure and decentralized identity management system for vehicles and their owners. This can help to prevent identity theft and fraud, as well as provide a secure and trusted platform for vehicle registration and ownership verification.

- **Secure communication**

Blockchain technology can provide a secure and tamper-proof communication network for vehicles and other IoT devices. By using blockchain, vehicles can securely communicate with each other, as well as with other devices in the IoV ecosystem.

- **Data privacy**

Blockchain can provide a secure platform for the storage and sharing of vehicle data. By using blockchain, participants can control who has access to their data, reducing the risk of data breaches and unauthorized access.

4.4. Smart Contracts

Blockchain technology enables the use of smart contracts, which are self-executing contracts that automatically enforce the rules and terms of a transaction. By using smart contracts, participants can automate the verification and validation of transactions, reducing the risk of errors and fraud.

- **Immutable Record**

Blockchain provides an immutable and tamper-proof record of all transactions, which can help to prevent fraud and other security threats. By using blockchain, participants can verify the authenticity of transaction data, reducing the risk of tampering and other malicious activities.

- **Distributed consensus**

Blockchain uses a distributed consensus mechanism to validate transactions, ensuring that transactions are validated by multiple parties and reducing the risk of fraudulent activity. This can help to increase the security and trustworthiness of the IoV ecosystem. Blockchain technology has the potential to improve the security of the Internet of Vehicles by providing a secure and decentralized platform for storing and verifying transaction data, as well as enabling secure communication, data privacy, smart contracts, immutable record-keeping, and distributed consensus. By leveraging the security features of blockchain, the IoV ecosystem can become more secure and trustworthy, reducing the risk of fraud, cyberattacks, and other security threats.

4.5. Blockchain Contributions in IoV-Assisted Smart Grids

The integration of blockchain technology in IoV-assisted smart grids has the potential to bring numerous benefits, including increased security, transparency, and efficiency. Figure 11 presents the most convincing arguments for using blockchain in IoV-assisted smart networks. Here are some of the key contributions that blockchain technology can make in IoV-assisted smart grids:

- Decentralization

Blockchain technology delivers a decentralized as well as distributed ledger that can facilitate safe and apparent transactions without the necessity for a central authority. This can help to reduce the risk of fraud, cyberattacks, and other security threats in smart grids [83]. Given that blockchain is founded on a decentralized framework that does away with centralized companies and third parties, it is an excellent choice for creating a more open and decentralized electricity market and trading system. Decentralized IoV connections, which also include more scattered elements like RSUs, automobiles, and people, may be created because to blockchain technology. These scattered entities can simultaneously handle their own operations on an independent basis [84].

- Trust and transparency

Blockchain provides a tamper-proof and transparent ledger of all transactions, enabling all participants to track and verify transactions in real-time. This can increase trust and transparency in energy transactions [85], as participants can be confident that their transactions are being processed fairly and accurately [86].

- Smart contracts

Blockchain technology permits the practice of smart contracts, which are self-executing contracts that automatically enforce the rules and terms of a transaction. This can help to automate the billing and payment processes in smart grids, reducing the need for intermediaries and increasing the efficiency of transactions [87,88].

- Energy Trading

Blockchain can facilitate P2P energy trading between consumers, allowing them to buy and sell excess energy to each other. This can help to balance the supply and demand of energy, reduce energy waste, and increase the use of renewable energy sources [89,90].

- Data Privacy

Blockchain can deliver a safe and private platform for the storage and sharing of energy information. By using blockchain, participants are in charge of who may access their data, decreasing the threat of data breaches as well as unauthorized access [91].

- Traceability

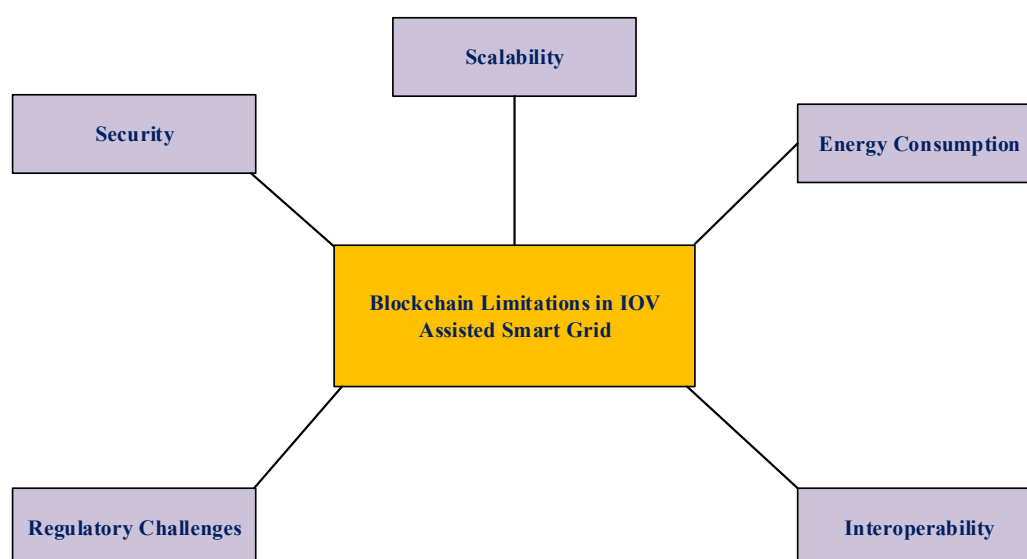


Figure 11. Restrictions of using blockchain in IoV-assisted smart grids.

Blockchain can provide a secure and immutable record of energy transactions, enabling participants to trace the origin and destination of energy flows. This can help to increase the

accountability and transparency of energy transactions [92,93]. Blockchain technology can bring numerous contributions to IoV-assisted smart grids, including decentralization, trust and transparency, smart contracts, energy trading, data privacy, and traceability. These contributions have the potential to increase the security, efficiency, and sustainability of energy transactions in smart grids.

4.6. Limitations of Using Blockchain in IoV-Assisted Smart Grids

The integration of blockchain in IoV-assisted smart grids has the possibility to improve the security, reliability, and effectiveness of energy transactions. Nevertheless, there are some limitations that must be addressed before blockchain can be fully implemented in smart grids. Figure 10 illustrates the constraints in the areas of blockchain as well as IoV-assisted smart networks. Here are some of the key confines of implementing blockchain in IoV-assisted smart grids:

- Scalability

One of the major restrictions of using blockchain in IoV-assisted smart grids is scalability. Smart grids generate large amounts of data and require high transaction processing rates, which can put a strain on the blockchain network. As the number of participants in the network grows, the processing time for each transaction increases, leading to slower transaction speeds [94].

- Energy Consumption

Blockchain technology is highly energy-intensive, and the energy consumption required for mining and verifying transactions can be significant. This can be a challenge in IoV-assisted smart grids, where energy efficiency is a key requirement. Therefore, developing energy-efficient blockchain protocols is necessary to overcome this limitation [95].

- Interoperability

Smart grids rely on the integration of multiple devices and systems, which can make interoperability a challenge. Different devices and systems may use different communication protocols and data formats, which can make it difficult to integrate them with blockchain networks. Addressing interoperability challenges requires standardization efforts and the development of protocols that can be easily integrated with existing smart grid systems [96].

- Regulatory challenges

The implementation of blockchain in IoV-assisted smart grids may raise regulatory challenges due to the decentralized and autonomous nature of blockchain. Smart grids are subject to regulatory requirements that may conflict with the blockchain's decentralized nature. For example, blockchain-based energy trading may require regulatory approval and compliance, which may not be easily achieved [97,98].

- Security

While blockchain technology is generally considered secure, there are still security concerns that need to be addressed in IoV-assisted smart grids [99]. One of the key concerns is the possibility of a 51% attack, where an invader gains control of the bulk of the blockchain network's computing power, allowing them to manipulate the network's transactions.

5. Driver Identification Data

Obtaining sources of data for drivers has been the subject of various studies by researchers. The identification of drivers may be done using a variety of data sources. As illustrated in the below Figure 12, the primary data sources may be divided into the following three groups: on-board sensor data, driving simulator data, and biometric data.

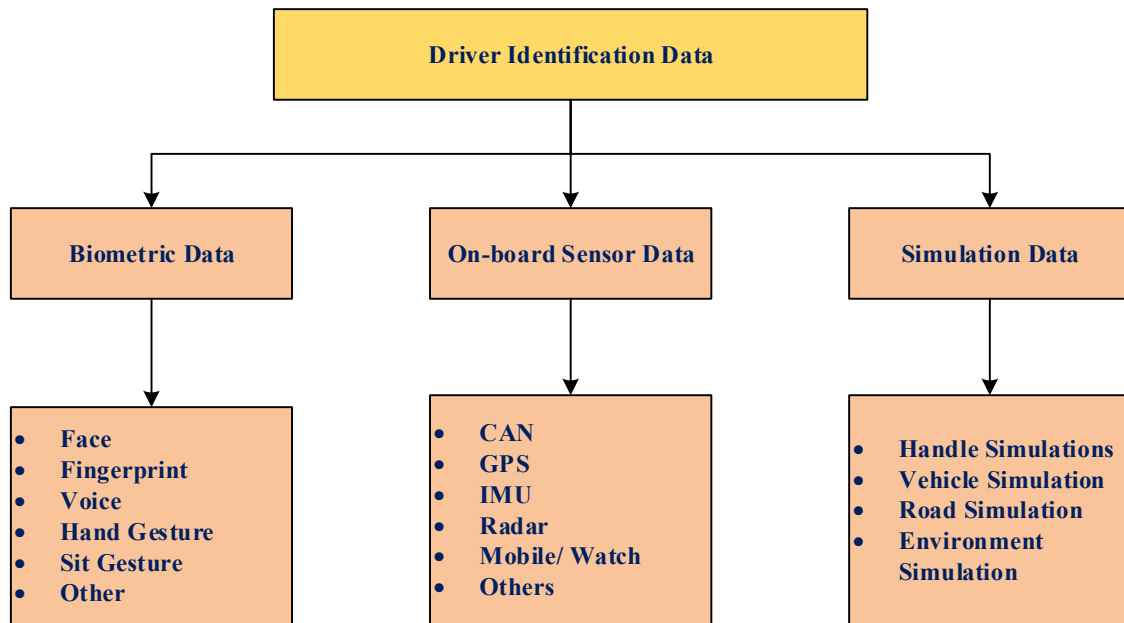


Figure 12. Data classifications for driver identification.

- **Biometric Data**

In identifying drivers, some studies employ driver biometric information. Commonly used terms include face, movement, fingerprints, audio, condition, gesture, and grip posture [100]. With great precision and significant pertinence, these data can accurately and immediately depict the driver's physical attributes. However, the current issues are that new equipment is often needed to capture data, leading to several issues including space occupation and increased costs. At the same time, there have been challenges with ongoing real-time identification, data collecting that invades individual privacy, and software restrictions such as simple data fabrication [101].

- **On-Board Sensor Data**

As sensor technology, on-board CAN software, networking communication technology, and intelligence terminals have all advanced quickly, numerous on-board sensor devices have gathered enormous amounts of high-quality, accurate, and objective data in actual driving situations. Relevant researchers have shown a considerable deal of interest in such data since they offer rich information that may be required to analyze the driver [102]. Smartphones, smart watches, navigation systems, and IMU data [103] are examples of common data from on-board sensing devices. The on-board CAN bus data have evolved into the primary data source for driver identification as a result of the integration of CAN technology in current automobiles. Some scholars have had success identifying drivers using the on-board CAN bus data [104,105].

Another type of on-board sensor information used to recognize drivers is GPS data. One may get GPS data by utilizing a common portable device or the on-board navigation system. It provides real-time functionality, high scalability, good practicability, and a low purchase price. To identify drivers, some studies utilize GPS information. Researchers have concentrated on driver identification by collecting data from built-in sensors on mobile terminals such as smartwatches and smartphones due to their prominence [106,107].

In conclusion, several data sources may be utilized for driver recognition, and each type of data has distinct properties; Table 1 lists the pros and cons of several types of data. On-board sensors can be utilized to actively and continually confirm the identification of the driver while driving with no negative influence on individual privacy. They have high efficiency, dependability, and safety, and they are increasingly replacing other methods of identifying the driver.

Table 1. Strengths and weaknesses of various types of data.

Data	Biometric Data	Driving Simulator Data	On-Board Sensor Data
Strengths	Simple, direct special sensor, high accuracy Easy to implement	Easy to do the test again with the ability to manually design driving situations and collect data on various working conditions.	Unbiased and realistic driving scenario and the information is reliable, accurate, and difficult to fake. Good real-time data at a reasonable price without compromising privacy.
Weakness	Built-in sensor surges hardware cost, and the device needs to manually activate image intrusion into personal privacy.	Distinct from actual operational circumstances, and the price of test facilities is not expensive for data accuracy.	Data gathering over the CAN bus protocol needs authorization and a significant expenditure in constructing a database.

- **Driving Simulator Data**

The capability of using driving simulation to acquire information on several working circumstances such as roads, traffic, and weather situations has great flexibility; however, the leading drawback is that a driving simulator has restricted capacity to replicate and capture the actual driving circumstances, and the driving simulation info may not match the actual driving data [108].

5.1. Driver Identification Models

Figure 13 depicts the categorization of driver identification techniques into three groups based on the properties of the models: deep learning model recognition, classic machine learning model recognition, and hybrid model recognition methods.

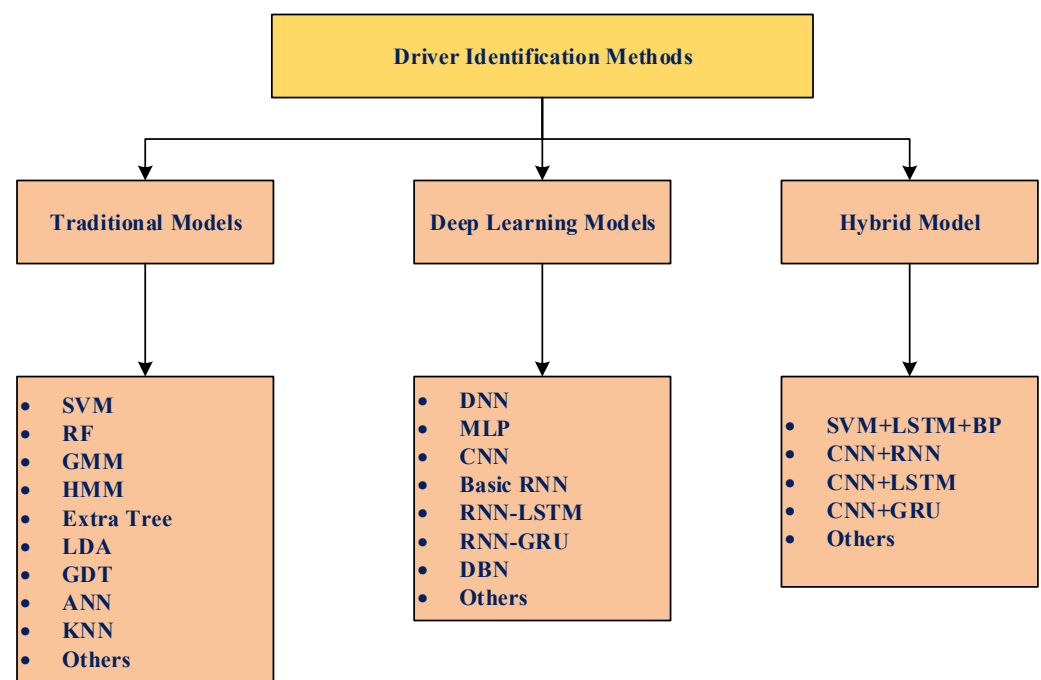


Figure 13. Categorization of driver identification techniques.

- **Traditional Model**

Machine learning is the process of deriving broad principles from scant observational evidence and applying these principles to forecast unlabeled data. In order for the typical ML model to forecast the outcomes of the output, the data must first be expressed as a collection of features before being fed to the predictions and classifier. The parameters have a significant influence on the identification accuracy of the model and are mostly dependent

on artificial experiences or the addition of new feature methods for extraction. SVM, RF, GMM [109,110], HMM [111], additional trees [112], LDA [113], GDT [114], ANN [115], and KNN [116] are examples of common models. The examination of the development of the application of SVM and RF models to detect drivers is the primary focus of this research.

- SVM Model

The SVM is a binary classification model. Its basic model is the linear classifier having the largest variation in the feature space. The fundamental idea behind the SVM classifier is to resolve the separation hyperplane with the biggest geometric interval and the ability to accurately split the training dataset [117]. SVM models have the potential to significantly improve a number of different areas of EV DWC systems. Using behavioral patterns or biometric data, SVM may identify and authenticate drivers or cars in real time for authentication and security purposes, ensuring that only authorized users have access to the charging infrastructure. In order to accurately authenticate drivers and enhance safety and personalization, SVM can assess data from driving behavior or biometrics for driver identification. Furthermore, SVM can identify abnormalities or flaws in the DWC system, enabling prompt interventions to preserve reliability. SVM can categorize and validate transaction data when combined with blockchain technology, enhancing the security and effectiveness of communications within the Internet of Vehicles (IoV) ecosystem. Because SVM can handle high-dimensional, complicated data, it is perfect for enhancing DWC system security and performance.

- RF Model

The RF model is a non-linear classifier that performs interactive educational training on samples using several trees to complete predictions. As seen in Figure 14, it creates a cluster classification model made up of several decision trees in random order. The RF model selects input variables and feature values at random to handle a vast volume of high-dimensional data. It features a low generalization error rate and good training efficiency. It is used by certain academics to pinpoint drivers. For instance, Hallac et al. [118] suggested identifying drivers with a 76.9% accuracy rate utilizing the RF model for CAN bus data acquired while turning and driving. The main problem with the RF model is overfitting in some challenging classification or regression operations. The findings mentioned above show that the classic machine learning model's recognition accuracy is typically within 90% and that the input dataset and design choice have a significant impact on this accuracy. This is mostly caused by the use of manual extracting features in standard machine learning techniques, the inability to capture complicated temporal aspects, and the poor capacity to fit high-dimensional nonlinear data. Big data samples are also challenging to enter.

- Deep Learning Model

The artificial neural network is where the deep learning technique has its roots. It is a method of computing that stacks several nested loops before processing the result one layer at a time. It converts the input representations, which are not deeply linked to the output objective, into higher-order data augmentation. In 2016, this technique was attributed partly to the task of identifying drivers, and it performed well in terms of identifying and describing prospective driving behaviors. With the growth of big data and cloud computing, as well as a significant increase in computer power, the deep learning approach has been successfully applied to map driving info to distinctive features of drivers in order to recognize drivers. CNN, RNN, and MLP [119] are common models. The investigation of driver recognition techniques using CNNs and RNNs is the central subject of this work.

- CNN Model

Deliberately designed to analyze data with an identical grid layout, a CNN is considered a neural network that enhances a DNN with a convolutional network to efficiently extract features. It has the attributes of shared weights, local connection, and automated extraction of features. CNN is limited in that it cannot represent modifications in time series, though. A convergence layer, a layer, and complete connection layers are cross-stacked to

create the CNN. To recognize handwritten digital images, LeCun et al. [120] developed the first CNN model in 1998. The difficult part of the driver identification process is identifying and extracting the essential characteristics of each driver's distinctive driving style. This is a smart approach, since a CNN can autonomously extract characteristics from driving data. The prediction accuracy might reach 80% in just 4–5 min, according to the real-world car test. To identify drivers and extract attributes relevant to driving behavior, Azadani et al. [121] employed a CNN as an input and feature data such as speeds, accelerating, and steering wheel orientation as outputs. Real-world driving data from 95 individuals were used to evaluate the model, and the findings revealed that the deep learning algorithm performed very well indeed.

The CNN method is superior to the conventional machine learning approach in that it employs the original signal peptide of car CAN bus information as an input and achieves an overall accuracy of 99.3%. CNN has the drawback of being unable to obtain the long-duration time aspects of the dataset and can only catch local time properties according to the length of the convolutional kernel.

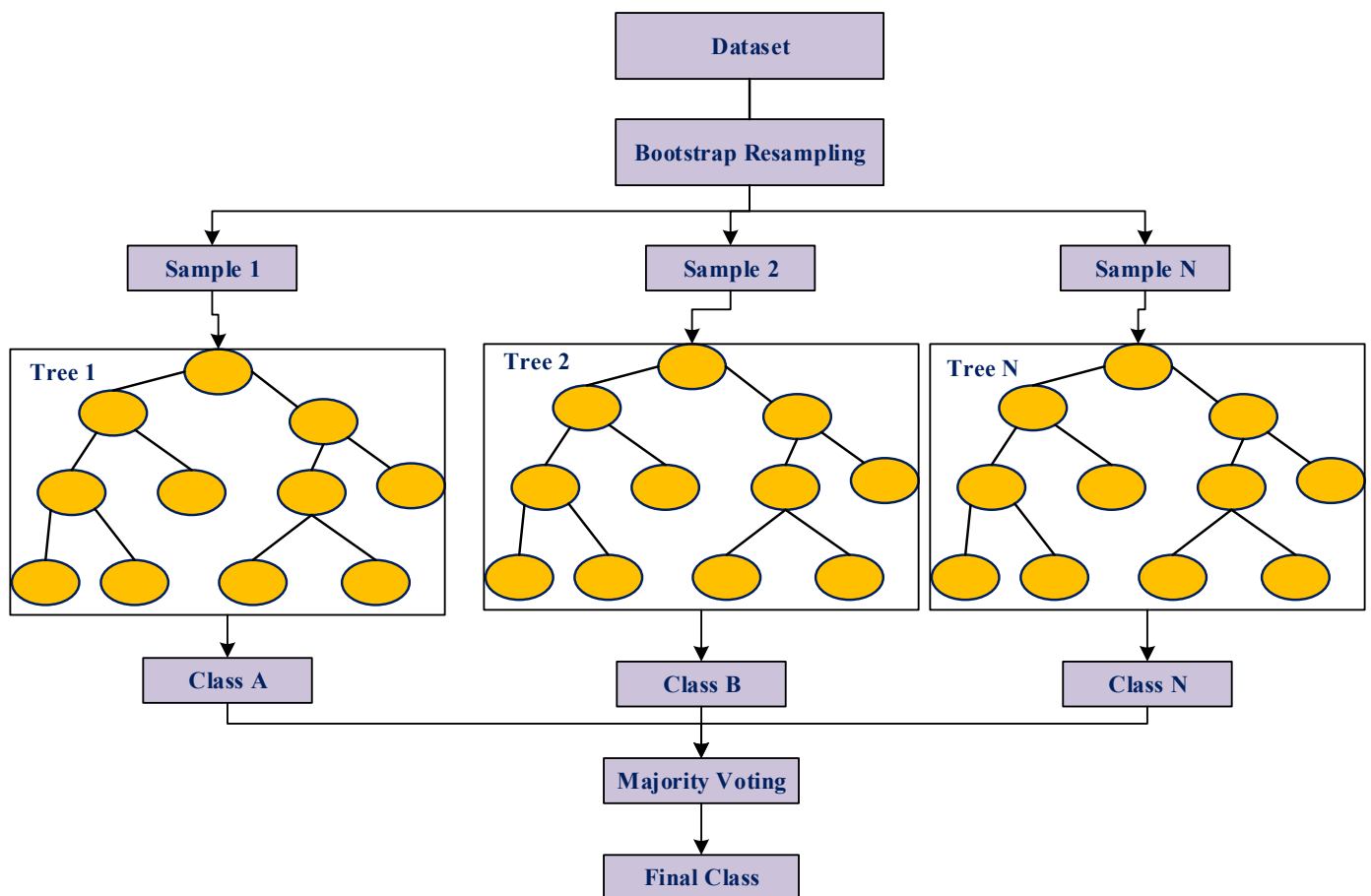


Figure 14. The RF model's guiding principle.

- RNN Model

A neural network with the capacity to store time information is the RNN model. The data input that its neurons may absorb includes both external information and internal information. The interplay between the information received then and the rest of the time generates the output of its neurons. Input, hidden, delay, and output layers, as shown in Figure 15, make up the network topology of the fundamental RNN, which has a loop. The fundamental RNN is capable of modeling time-series data, but it suffers from gradient disappearing and explosion brought on by long-term dependency.

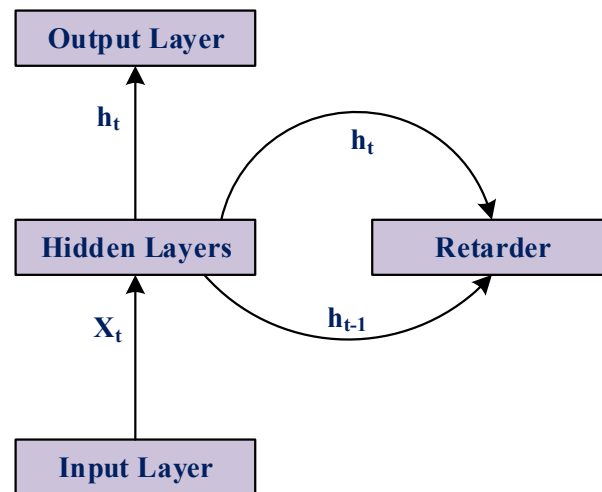


Figure 15. Structure of RNN.

- Hybrid Model

Numerous researchers have tried to use hybrid models to even further enhance the accuracy of driver detection in order to fully use the benefits of various fundamental models. The hybrid model is classified down into compound type, series type, and parallel type in this study. For driver detection, several studies have employed the serial hybrid method. For illustration, Zhang et al. [122] created a hybrid model by stringing together CNN and RNNs and using the data from the vehicle’s CAN bus to identify the driver. The precision of recognition is approximately 98.36%. As per Moosavi et al. [123], a hybrid model should be created by stringing together a CNN and an RNN. The CNN should be utilized to extract the semantic patterns of driver performance from the vehicle’s CAN data, and the RNN should be utilized to classify the driver’s preferred driving techniques. Several scholars used hybrid parallel models to determine drivers. For instance, Mekki et al. [124] suggested a hybrid model for driver identification by simultaneously feeding simple and multivariable time-series driving statistics into the CNN and LSTM. The driving data series’ temporal correlation is what the model understands. The built-in driver identification model has a high level of resilience and generalizability, and its accuracy can touch 95%. To increase detection performance and accuracy, Hammann et al. [125] suggested a hybrid model built from RESNET and LSTM running concurrently (as shown in Figure 16). The detection performance of five drivers on the database Utdrive achieved 96.90% using this model.

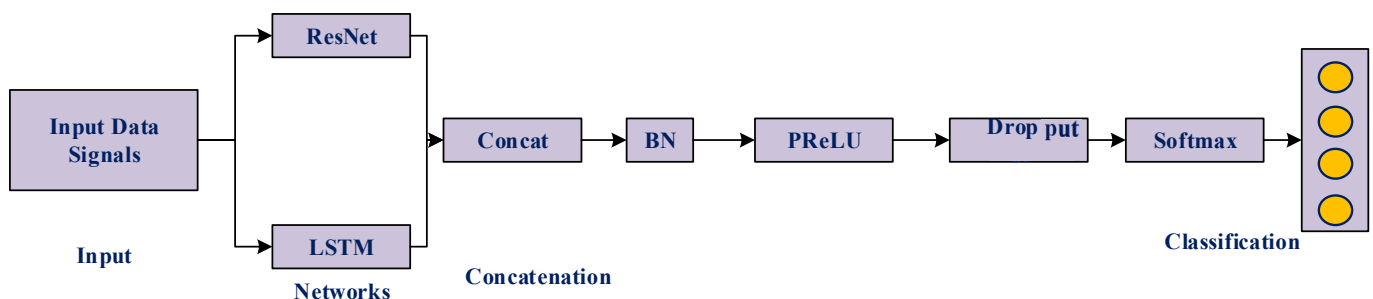


Figure 16. The hybrid model used by Hammann et al. [126].

A few pieces of research show complex hybrid models. For example, Moreira et al. [126] produced a driver detection technique by combining integrated hybrid models from LVQ, RF, SVM, and boosted C4.5, significantly lowering model generalization errors (as shown in Figure 17). Jafarnejad et al. [127] recommended a hybrid model structural design made up of integrated modules and also an RNN layer that uses GPS movement data attributes

to identify drivers. In the case of between 5 and 100 drivers, the identification accuracy is between 86.5% and 98.1%. With a hybrid network model built by Sánchez et al. [128] using Resnet-50 and also the GRU, the maximum driver recognition accuracy was 92.02%.

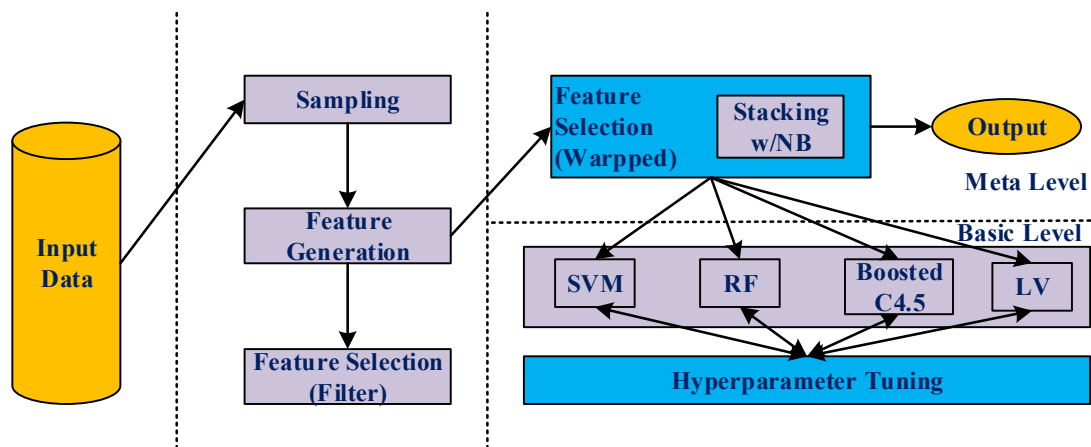


Figure 17. The hybrid model pre-processing and model introduction.

In summary, the hybrid model can choose the fundamental model in accordance with the objectives and data available and design various model configurations or learning networks with various width and depth structures to enhance the precision, reliability, and real-time efficiency of driver identification. The three forms of identification models have been analyzed above, and it is clear wherein each category of the model has unique functional properties. The manual choice of attributes has a considerable impact on the precision of the standard machine learning model, which typically requires extracting the statistical aspects of the data using specialized knowledge. The comparison of feature data as well as the length of the tester data have a significant impact on the DL model, which needs a huge sample size of info and has attributes like feature extraction, seamless ability to connect with the classifiers, high precision, and huge computational resources and power occupation. The hybrid model has great generalization and resilience capabilities and fully exploits the benefits of many models.

5.2. Summary on Driver Identification Technique in EV

The driver identification technique is a significant study area in the creation of intelligent cars and vehicles and cutting-edge transport networks and is crucial in scientific disciplines like traffic safety and driving support. The evolution of driver detection methods is examined in this research. The article's important contents include assisting future researchers in conducting in-depth studies of driver identification systems, serving as a reference for additional data collection research, suggesting a possible solution to assist researchers in creating models with performance improvement, and providing insightful data on technological trends to advance research into electric vehicles.

In addition, this study breaks down the fundamental phases of the driver detection step into four categories: data sampling, driver recognition, data processing, and technical application. Data collection and model development, the two crucial components of the driver identification process, are examined and addressed. It is demonstrated that the on-board sensor info includes valuable information and may be utilized as the primary data source for detecting drivers by contrasting and examining the benefits and drawbacks of various types of data. It is determined that the DL EV model has benefits over the conventional ML model in terms of recognizing robustness and accuracy and will eventually replace it as the go-to technique for accurate driver identification by examining the research improvements of the three different ML models—deep, traditional, and hybrid. It is also validated that the hybrid model can rationally choose models in accordance with the activity target and data needed, allowing it to fully capitalize on the benefits of various

models in order to further enhance generalization ability and identification robustness, as well as having a promising future.

Despite considerable progress in the efficiency of driver recognition, there continue to be numerous studies that need to be done. The methods for identifying drivers have advanced considerably, as seen in the explanation above. Yet, in actuality, because it is a continuously connected system, numerous things might affect its quality. Driver authentication programs on the web still need to develop in terms of computing accuracy and efficiency, among other things. Firstly, the abundance, complexity, and variety of driving situations all have a significant role in how reliable the driver identification system is. Vehicle on-board multi-sensor data has progressively replaced other sources as the primary data source for driver recognition with big props to qualities like objective reality, precision and reliability, large amounts of data, no intervention for the driver, safeguarding individual privacy, and less financing costs. Data label automated labeling technology and data enhancement generating technology have grown into significant methods of enhancing data. The driver identifying the system's accuracy, real-time efficiency, and resilience are all improved by the combination of software and hardware technologies. To improve vehicle and traffic safety, academics must keep doing in-depth, precise theoretical study as well as applied research on driver screening methods.

6. Standards, Protocols, and Emerging Technologies for EVs

There is a growing need for charging points since EVs have emerged as a crucial component of the transportation infrastructure. Protocols are standards and procedures that provide efficient data transfer and interaction between different organizations in the EV business. Administrators and service operators of charging stations have difficulties with the procedures and rules governing their platforms. In order to facilitate effective communication between multiple organizations, including plug-in EVs of plug-in, smart grids, and charging element stations, standards and protocols are utilized. To fulfill the ever-increasing EV expectations and necessities, several international organizations and research institutions have established and implemented both open-source and private networks. Interoperability constitutes one of the difficulties in the creation of plugin EVs. Battery BEVs are more popular, which presents problems with effective management of energy from the grid, management of the battery, and data transmission authentication. The entire EV protocols' parameters and specifics have already been released [129] by the Dutch innovation hub ElaadNL. Prominent standards and protocols for EVs have been deliberated in [94,95] and abridged in Tables 2 and 3.

Table 2. PEV industry standards use cases [129,130].

Standard/Protocol	Use Cases
Ocpp [129,130]	Billing, charging point operation, smart charging, charging session authorization, grid management, reservation
OChp [129,130]	Reservation, charging session authorization, providing charging point data, smart charging, roaming
OCPI [129,130]	Reservation, charging session authorization, providing charging point data, smart charging, roaming
OSCP [129,130]	Distributing capacity budgets, utilizing these budgets to manage grid capacity, and smart charging by sharing capacity projections
OpenADR [129,130]	Smart charging, managing grid, handling registrations
eMIP [129,130]	Charging session authorization, roaming, facilitating smart charging features, billing
ISO15118 [129,130]	Schedule-based charging, charging session authorization, certificate handling
IEEE2030.5 [129,130]	Solutions for n-house smart grids, requesting action and load management, sharing metering information, publishing tariff details, text message sending, giving information on real consumption and invoicing, and reservation for energy flow.

Table 2. Cont.

Standard/Protocol	Use Cases
IEC61850 [129,130]	Modeling of communication parameters, uniformity of message format, plug-and-play functionality for a variety of applications, including coordinating EV charging stations and operating virtual power plants.

Table 3. Use cases of various EV standards and protocols [131].

Use Cases	OCPP [131]	OCHP [131]	OCPI [131]	OSCP [131]	Open ADR [131]	eMIP [131]	IEEE 2030.5 [131]	IEC 61851 [131]
Manage Grid				*	*			
EV Charging								*
Handle Registration			*		*		*	
Billing	*	*	*			*		
Provide Charge Point Info		*	*			*		
Smart Charging			*	*	*		*	
Roaming		*	*			*		

The V2G sector of the economy is still developing. When efficiently integrating EV features into the management operations of the grid, the protocols standardization is essential for addressing novel needs of the EV communications set-up [132]. The operation of IEEE 2030.5 [133] has previously been modified to include CA Standard 21 [133] and IEEE 1547-2018 [133]. This is a web services-based application level standard featuring built-in privacy that is intended to utilize the current network to convey its communications across devices. It is quickly becoming the DER messaging industry standard [133]. The IEC is working to define a number of standards for the DC rapid charging option. The criteria for grid connections and communication architecture for rapid charging are represented by the IEC 61851-23 standard [133]. In Table 3, numerous message protocols and standard use cases for EVs are shown.

The IEC 61850 protocol has also been updated often to include EVs as well as their associated activities [134]. To effectively handle an ad hoc fleet of vehicles and the billing load, attempts have been made to link several protocols, including IEC 61850 [135] and IEEE WAVE [135]. Even though ad hoc networking across multiple EVs has prompted privacy issues, the early findings have been quite encouraging. Investigations on protecting these information exchanges have been conducted in order to solve these worries. The IEC 61850 connectivity of EVs in a network is handled by XMPP in [136], another endeavor that associates standard harmonization and resolving safekeeping distresses. By the use of hardware-in-the-loop testing, whereby standard instructions are transferred to carry out for controlling power systems, such methods have additionally been examined in real-world testing circumstances. IoEV focuses on tying up EVs online to regulate and coordinate energy and data transmission for V2X. Several standards are being developed or have already been published, because this is a developing field. The SAE has established a set of networking protocols and standards that the EV must adhere to when it is being charged. In [137], prototypes for grid power management, EV, PV, and household energy management systems are developed based on IEC 61850. Moreover, communication information channels have been developed, and their effectiveness has been assessed using a variety of communication methods. According to simulation results, [138] Hussain et al.'s technique of using cognitive radio to enable a connection during contingencies is feasible.

6.1. New Communications Technologies for Electric Vehicles

During the past several years, the volume of autonomous vehicles has substantially expanded. Autonomous cars and smart cities both rely on effective and dependable V2X communication. Architectures that are low-latency and energy-efficient must be used to achieve V2X communication [139]. Figure 18 shows an example of V2X communication between a vehicle and a passenger, network, vehicle, and infrastructure. Data interchange from automobiles to those other devices at great speed avoiding data packet loss is the major problem in V2X communication. The other equipment, as well as the technological components of the car, must quickly reply to requests issued by each other. For V2X communication, innovative technologies including IoT, LoRa, and 5G are frequently employed. For EVs, the IoT offers a number of benefits and flexibility. Several writers have suggested numerous IoT-based charge management system types. For the purpose of coordinating the charging of large-scale vehicles in multiple residential complexes, a better-decentralized charging system is suggested [140]. To extend the lifespan of EV batteries, a precise charging status estimation is required. It has been suggested to use the Coulomb technique as well as MQQT for connectivity in a battery management system [141].

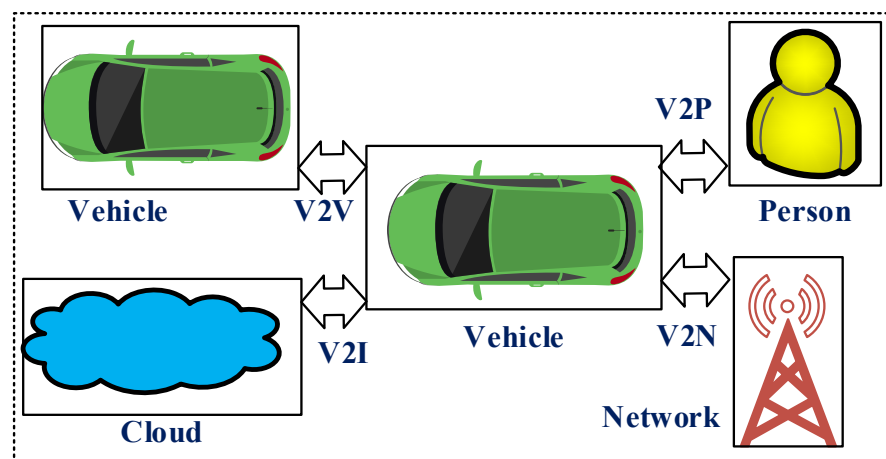


Figure 18. V2X communication of EVs.

IoT facilitates V2V and vehicle-pedestrian connection. For sending messages from one machine to another or from a machine to a person, MQTT and COAP protocols are frequently utilized. The three main components of IoT are bidirectional communication, data collection, and response management. Standards for wireless and wired communication include cellular, LoRa, BLE, Wi-Fi, and Zigbee. Table 4 provides a comparison of the characteristics of several communication systems.

Table 4. Common communication protocols employed in IoEVs [142].

Communication Technology	Standard	Speed	Range	Frequency Spectrum
Zigbee	IEEE 802.15.4 [142]	250 Kbps	100 m	2.4 GHz
LoRa/LoRaWAN	IEEE 802.15.g [142]	27 Kbps	10 km+	865–926 MHz
WiMAX	IEEE 802.16 [142]	70 Mbps	50 km+	2–11 GHz
Wi-Fi	IEEE 802.11 [142]	100–250 Mbps	100 mts+	2.4, 5 GHz
GSM/GPRS	ETSI	114 Kbps	35 km+	1800, 1900, 900 MHz
LTE	3GPP	0.1–1 Gbps	28 km/10 km	700–2600 MHz

Frameworks and architectures built using the aforementioned technologies have been offered by several authors. Using EMU, customers may view their energy use. EMUs assist users while interacting with the electricity grid. EMU communicates with EVSE using WLAN as well as Zigbee (802.15.4). Zigbee is a comprehensive solution used by the majority of smart home environment vendors [143].

Facilities for smart grid programs are available through mobile communications with several carriers. To facilitate garage charging, EMU as well as power meter makers integrate digital communication devices. Application data are transmitted at regular intervals, including pricing and energy usage statistics. The most well-known mobile networks provide a number of benefits: Since about all mobile networks utilize licensed spectrum, it is not necessary to use unauthorized bands of the frequency range, and all mobile networks are fairly configurable in order to link numerous EVs, cellular communication technologies like 5G are sufficiently forward-looking to encounter the needs of smart grids. The discussion of numerous trends, possibilities, and modeling techniques for LoRa technology was done by Mukarram A. M. Almuhtaya et al. [144]. For the purpose of evaluating the LoRa/LoRaWAN efficiency of the system, the writer examined widely used simulation tools. The LoRa/LoRaWAN efficiency was also categorized by the authors according to network throughput, network availability, energy usage, service quality, and privacy.

Wi-Fi is being used by charging points to provide wireless communication among the electric car, the customer, and the equipment for charging, transforming them into far beyond a simple charger. In both wireless and wired charging environments, Wi-Fi is increasingly the most efficient way to manage the charging flow [145]. The development of electrical vehicle applications has made considerable use of wireless communication protocols like Zigbee and LoRa. Examples of these applications include the modeling of EVCS, system configuration for the EV smart charging network, and adoption of SEM with the help of the network of LoRa.

6.2. Computational Technologies Intended for EVs

The past several years have seen a transformation in numerous industries, including the healthcare system, education, military, finance, farming, and banking, thanks to computing technologies like big data, artificial intelligence, and block chain. Several datasets have indeed been subjected to the use of AI technologies like deep learning and machine learning for forecasting and anticipating outcomes. AI has a part or subset called ML that imitates human behavior. Labeled data may be analyzed using supervised ML techniques such as classification and regression. In biology, a part of science and focused marketing applications, untrained ML techniques including dimension reduction, correlation, and grouping known as clustering are widely employed. The use of reinforcement algorithms in car navigation applications is widespread. Robotics for factory automation typically uses reinforcement learning methods.

A subclass of AI called deep learning methods may be used on unstructured information to enable computational methods to gradually learn characteristics from information at different stages. In ADAS, deep learning methods are widely applied. Researchers utilize programs like PyTorch, Tensor Flow, and Keras to develop applications for deep learning. Big data refers to vast quantities of complicated, difficult-to-manage, organized, and unstructured data that are either impractical or impossible to analyze using conventional techniques. With the expansion of IoT, smart meters, RFID tags, and sensors are producing enormous amounts of data, necessitating data analysis and interpretation. Big data analytics and processing are commonly carried out using specified tools like Apache Spark as well as Hadoop. Blockchain technology keeps track of all payments in a digital ledger that cannot be altered or compromised [146]. As a new payment occurs, the entry is recorded in the recipient's digital ledger. It is a distributed ledger system that records transactions using an unchangeable cryptographic sign known as a kind of hash. The most

well-known digital coins that employ blockchain’s distributed ledger system are Ethereum and Bitcoin.

6.3. ML for Plug-In Electric Vehicles

A common subclass of artificial intelligence used in applications for computer vision and data science is machine learning. Applications for EVs may benefit from the efficiency that makes them successful by utilizing machine learning technologies. As EV shipments have risen quickly, setting up infrastructure like EVSE and properly controlling EVs is difficult. EVs are preferred because they are energy efficient. EV management and coordination may be done using machine learning technologies. As shown in Table 5, there are three different categories of algorithms used in machine learning: supervised, unsupervised, and reinforcement. Figure 19 depicts the procedures needed to apply ML algorithms to EVs.

Table 5. Various ML types.

Types of ML	Purpose
Supervised	Regression, Classification, Forecasting
Semi-supervised	Labeled as well as unlabeled data
Unsupervised	Clustering, Association, and Dimensionality reduction
Reinforcement	RNN, ANN

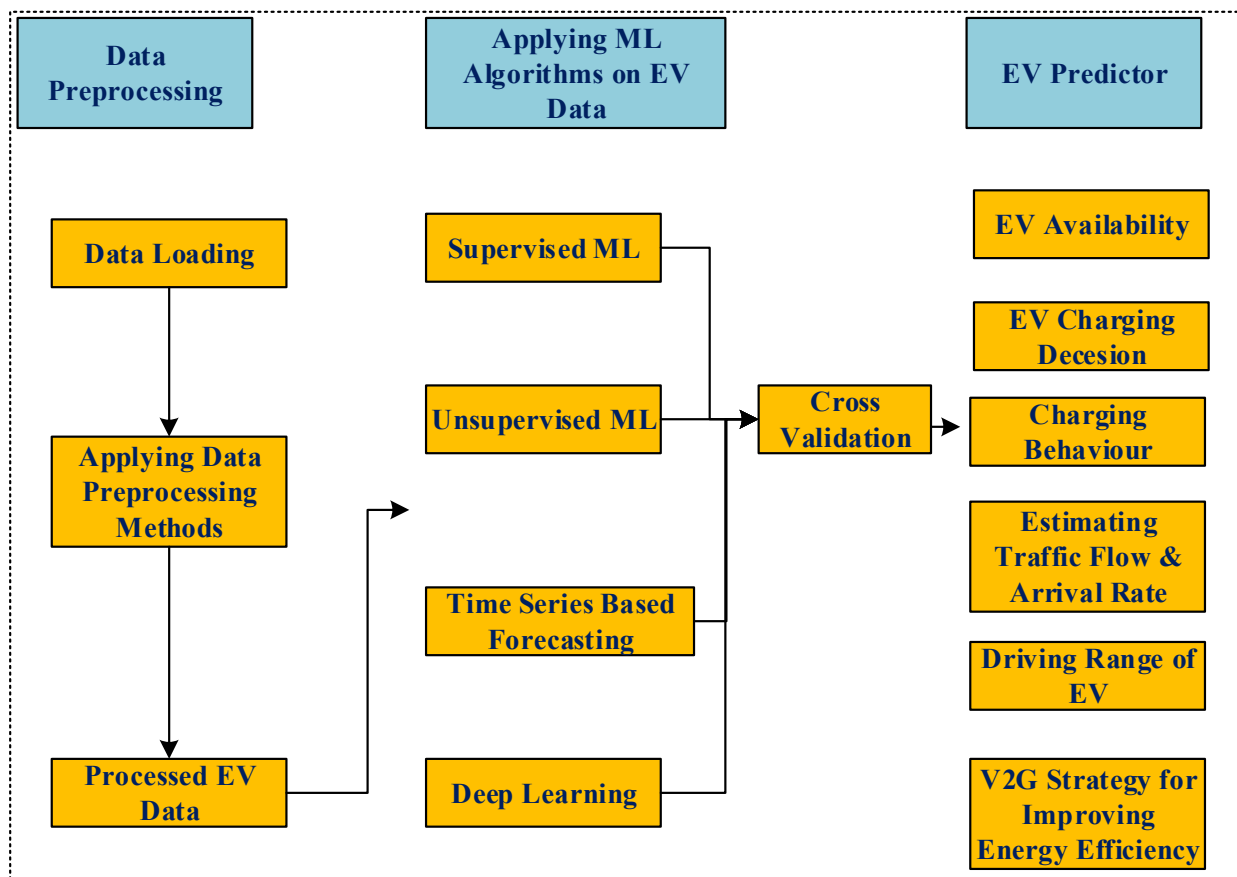


Figure 19. Implementing ML algorithms for forecasting EV.

For load prediction, unsupervised ML techniques including k-nearest neighbors, decision trees, and random forests were utilized. The estimated driving distance of EVs is unreliable, and hence an improved BMS is needed to determine how much power is still available for additional travel. To accurately anticipate the driving distance of EVs, Yong Wanga et al. suggested the LGBM. The characteristic significance scores are given in this method in order to determine the link. A model was put out by Donovan Aguilar Dominguez et al. to forecast when an EV offering vehicle-to-home services will be available [147]. In order to forecast the accessibility of EVs, ML algorithms have been used for data pertaining to various car usage profiles, defined by the count of trips done each week. On the basis of a Bayesian-based probabilistic model, Rafael Basso et al. suggested time-dependent EV scheduling problems with chance limitations [148].

6.4. Big Data Technologies for EVs

Big data is the term used to refer to the enormous volume, complexity, and wide variety of information that is challenging to analyze by conventional means. Big data includes unstructured information, including text files, emails, movies, and audio files [149]. The adoption of carbon-free commuting has been significantly impacted by EVs. Data are created from a variety of sources, including onboard as well as off-board sensors of different infrastructures, which are communicated with by PEVs. EVs are indeed generators of this data. Big data may be utilized to create algorithms, siting plans for charging outlets, and different BMS rules after it has been saved in cloud servers. Big data technology makes it easier for EV producers and governments to seize these chances. Organizations are capable of determining the number of EVs utilizing nearby charging stations thanks to real-time recharge data from EVs. Peugeot and IBM joined together to provide new associated car facilities, such as analyzing driving data to benefit merchants and auto dealers. Peugeot can examine a variety of vehicle and driver data for secure transportation thanks to IBM's big data and analytics technology. In smart urban areas, the data obtained can help decision-makers with road construction and reduce traffic congestion [150]. Driving circumstances may be adjusted for any hazardous situations avoided with the use of streaming data.

Every $2x$ years, where $x = 1, 2, 3, \dots, n$, the amount of data doubles. The velocity, variety, and volume of data have expanded as a result of recent IoT developments. Big data is a result of the enormous quantity of data produced by structures, electric vehicles, and smart grids mostly with the fastest data transfer speeds. Table 6 lists the distinctions between conventional and big data. Novel analytical methods are used with vast, diverse datasets that comprise varied amounts of structured and unstructured data from multiple sources in big data analytics. Huge amounts of data are generated as a result of the continual transmission and receiving of information from the infrastructure, passengers, other cars, and other sources via various sensors both within and outside the automobile. To effectively use this massive data, sophisticated data analytic techniques are needed in order to extract insightful and valuable information. The two big data analytics solutions that can be used to address future big data difficulties are Hadoop and Apache Spark [151]. To manage the enormous amount of data produced by ESEVs, intelligent electronic devices, and smart meters, big data analytics is required. Each EV has sensors and electrical components that track the battery's operation and charge level.

Table 6. Difference of big data and conventional data.

	Big Data	Conventional Data
Data Type	Structured, unstructured, semi-structured	Structured
Data Structure	Distributed	Centralized
Data Relationship	Complex	Uncertain
Data Volume	Petabytes and zettabytes	Terabytes

Several technologies may be used to store and evaluate the volume of information produced by diverse sources. Before employing the tools for gaining insights, it is important to differentiate between big data and regular data. Big data and conventional data are used with different techniques and instruments. Big data analysis may not be supported by analytical methods used for conventional data. Big data analytics and processing make considerable use of the Spark and Hadoop frameworks.

Huge data collections may be processed over computer clusters using Apache Hadoop, a robust and dependable distributed software system. The architecture is made to expand from one server to several servers, and the framework additionally recognizes and manages application layer errors. Modules like Hadoop Common, Hadoop YARN, HDFS, and Hadoop MapReduce are part of the Apache framework. The HDFS framework's shared file system, which has a maximum throughput, is its foundation. Large sets of data are processed in parallel while being managed by a cluster using MapReduce and Hadoop YARN. Ambari, Hive, Cassandra, Hbase, and other projects are among the others that are linked [152]. For working on data-science-related tasks on single-node clusters, Apache Spark is yet another well-liked framework. Apache Spark's main strengths include ML and SQL analytics, as well as real-time streaming information processing. For ad hoc and dashboarding reporting, Apache Spark could perform SQL queries fast. A variety of ML and analytics frameworks may be connected with Apache Spark. Hadoop works well for batch processing because it uses the MapReduce capability to split huge datasets among clusters for computing in parallel. In contrast, live broadcasting data analysis makes considerable use of Spark. The security features of Apache Hadoop include LDAP, ACLs, and more. Hadoop provides essential protection for Spark. The big data of electrical vehicles are made up of information from PEVs, charging stations, and infrastructure, and it has to be analyzed using big data analytic software that runs across a cloud service. The charging status of the car may be checked via smartphone applications created by automakers. Data are mostly produced by the vehicle's electronic components and sensors. Based on EV users' charging habits and tendencies, genuine government businesses can deploy charging stations using big data. For upcoming initiatives, enormous and diverse amounts of created data may be kept on the cloud.

Applications like battery monitoring, determining the best location for placing charging points, and checking PEV performance may all benefit from big data analytics. Big data analysis using conventional statistical techniques and algorithms does not yield relevant information. The absence of publicly accessible actual data regarding EVs and equipment is one of the problems with big data. For the direct contact of the electrical vehicles with the remaining infrastructure, effective and safe data analytics methodologies and technologies are needed.

6.5. Blockchain Technology for Electric Vehicles

A blockchain eliminates the need for a centralized authority to authenticate payments among two or more entities by distributing a digital ledger over a public or private computer network. The ledger will then be updated when each transaction has been computationally encoded, confirmed by many arbitration methods, and inserted as a new part of the record chain. Vehicles that utilize blockchain technology may process payments quickly. A hash known as SHA 256 is utilized to capture blockchain payments and to confirm the legitimacy of the transaction. Blockchain is a game-changing innovation in the fields of finance, medicine, and network security. The EV industry may be significantly impacted by blockchain technology [153]. Figure 20 displays the publishing data on the usage of blockchain for electric vehicles.

Furthermore, it has an upward trend, demonstrating its attractiveness for EV applications. Figure 21 depicts the whole blockchain infrastructure for EV applications. Making use of blockchain tools for EV-based applications will accelerate the growth of the EV sector. The blockchain design for EV infrastructure is shown in the upper diagram. In a blockchain network, V2X communications including vehicle-to-access-point techniques are frequently employed. Every mobile entity in the structure will have its own ID. Access or node points must be positioned at periodic intervals because they are the electronic components that can gather information from EVs. The EVs' integrated sensors provide data to the access points utilizing a variety of wireless communication methods on a continual basis. These characteristics include battery level, vehicle status, billing for recharging, and others. The records are viewed as blocks by the entry points throughout the blockchain system, and every access point should confirm the payment to maintain transparency. The transportation consultants connect to the blockchain system to continually monitor the state of the EVs and deliver to the EV owner individualized advice.

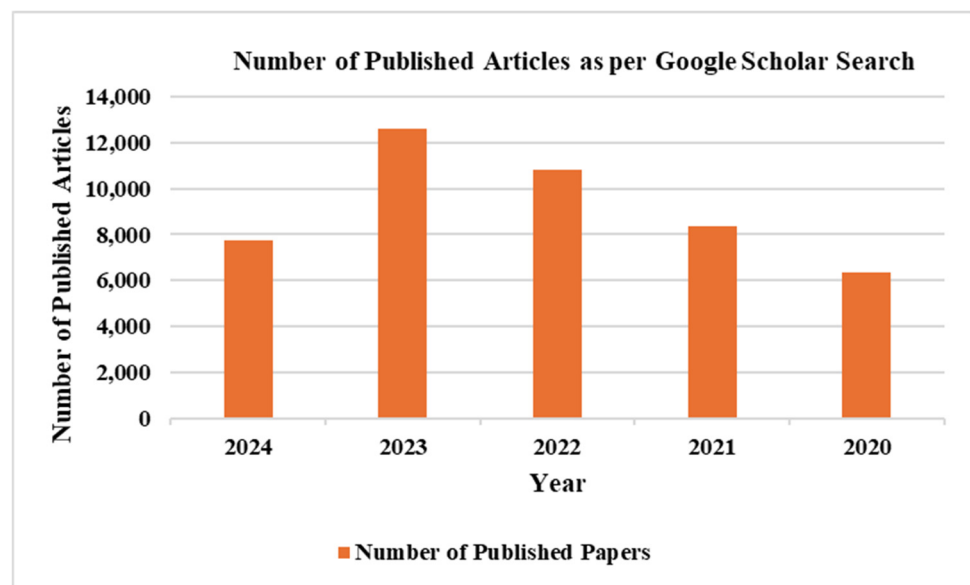


Figure 20. Publications on blockchain for EVs.

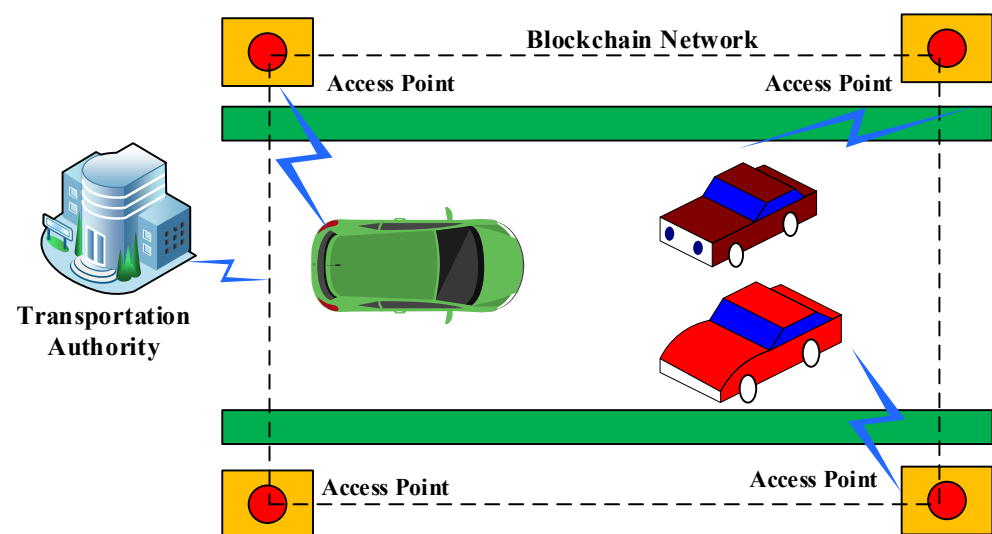


Figure 21. Blockchain network of EV transportation.

The advantages of implementing blockchain technology towards EVs include the ability to instantaneously verify payments through automated approvals and the processing of EV payments through the execution of contracts with the terminal based on the user's preference. Blockchain apps may be created on a variety of blockchain platforms. The prominent blockchain systems are shown in Table 7 [154] and include the Ethereum, XDC network, Hyperledger Fabric, Ripple, R3Corda, and others.

Table 7. Blockchain systems grouped by ledger and industry type.

Blockchain Platforms	Industry Type	Ledger Type
XDC Network	Cross-Industry	Permission-less
Ethereum	Cross-Industry	Permission-less
Hyperledger Fabric	Cross-Industry	Permissioned
R3 Corda	Financial Services	Permissioned
Ripple	Financial Services	Permissioned

Ethereum is considered a decentralized P2P blockchain platform that generates a network for safely running and validating software code, or “smart contracts”, over the internet. The Ethereum virtualized engine and Solidity programming language may be used to create incredibly adaptable decentralized applications [155]. The application code for smart contracts is built in Solidity as well as Vyper and is stored at a particular location on the blockchain. In Ethereum, a payment is defined as a verified data package containing a text to be transmitted from a third-party account. Upon Ethereum, apps that are both economic and semi-financial may be created. The first ever distributed platform to enable smart contracts created in Go, Node.js, and Java is Hyperledger Fabric.

Because the Fabric interface is permitted, players might not even entirely trust each other; however, a governance entity is based on the level of faith that exists among them. The pluggable administration identity methods used by Hyperledger Fabric include LDAP and OIDC. Blockchain technology may be used to solve issues including a lack of accountability in trade processes, according to [156]. In toll booths, blockchain may be utilized to handle payments automatically. E-wallets are being created by several businesses to process payments. PEV owners have the option of using smart contracts to supply surplus energy to charging points and using e-wallets or digital payments to pay their bills. Table 8 provides a comparison between Ethereum and Hyperledger Fabric.

Table 8. Comparison between the Ethereum and Hyperledger Fabric frameworks [157].

	Hyperledger Fabric	Ethereum
Private vs. Public	Private	Public
Governance	Federated	Decentralized
Permission	Permissioned	Permissionless
Smart Contract Languages	Javascript (Node.js), Java, Go	Vyper, Solidity
Private Transactions	Yes	No
Consensus Mechanism	Pluggable BFT	Proof-of-work
Speed	3000 Tps	15 Tps

Blockchain additionally enables producers to keep an eye on inconsistencies when raw resources for EV manufacturing are delivered to the facility. Some writers put forth frameworks and regulations for blockchain-based EV energy-selling platforms. For improved prediction and analysis with accountability, deep learning, and machine learning technologies could be used alongside blockchain knowledge.

6.6. EV Security Considerations

Because of their simplicity of use, EVs are presently utilized by a large number of individuals in city and semi-city locations all over the world. Throughout the last few decades, numerous automakers have been producing plug-in EVs. EVs emit little greenhouse emissions and cost less to operate and maintain. By reselling the power that is retained in their car's battery packs to the grid, EV owners may make money. The expense of battery packs, timing battery changes, access to charging stations while going to remote locations, and a strain on electric networks during peak charging times are all negatives of utilizing EVs. No matter whether it is a BEV or a PEV, every EV has a number of electrical systems and pertinent system software to communicate with the sensing devices and other equipment both within and outside of the car. To reduce the dangers associated with EV, both software and hardware protection is crucial. EVs may transmit signals and messages to other cars, passengers, and equipment to interact.

The linked devices come with some amount of danger. Connected vehicles use the Internet to transmit critical data further about drivers as well as other mobile units to an external infrastructure. Cybersecurity threats on connected vehicles grew seven-fold in 2019 [158]. The majority of connected and EVs depend upon embedded software to effectively manage and run the systems. An attacker can take advantage of security flaws to disable the brakes, take over the steering, and disable sensors, cameras, and ECUs, as well as access the private data of the equipment and other cars. The majority of connected vehicle and EV users operate navigation systems and other Bluetooth-related functions via smartphone applications, which could enhance the potential threat. Now, the biggest worry is the safety of EV battery charging. To interface with EVSE, an app is necessary for charging. The EVSE's constituent parts, such as firmware upgrades, physical connectivity, the line of connection between the EVSE and the car, and the mobile app are used by the driver of the car to monitor charging.

For EV protection, different automobile companies are using different coding protocols. The automobile industry uses ISO21434 [131] to lessen the risks associated with cyber security. It is difficult to minimize a few of the problems with cyber security concerns due to the intricate ecosystem of EVSE and EVs. The main difficulties are access and authorization control, individuality and connection management, and limits of the equipment and communication routes. A variety of threats against EV infrastructure, including rejection of service, latency attacks, and Sybil attacks, demonstrate a sociological, physical, and digital impact. By employing the aforementioned techniques, the attackers can disrupt connectivity on a more general or collective level. They can also create disruptions by demanding power at the wrong times, and they can duplicate ID credentials for a variety of uses. In order to secure data transfer between the charging point and the EVs, defense scientists have suggested authentication mechanisms. The authors of [159,160] covered several security-related topics, risks, and the risk paradigm in the EV charging network. The writers also contrasted several safekeeping methods that provide capabilities for invoicing, protected payment, and verification. A verification protocol that offers straight authentication procedures between several components was presented by Farooq et al. [161]. For EV charging networks, a method was created by Hamouid et al. The standard also offers other benefits like anonymous and quick verification in addition to hiding the position of the EV throughout the whole charging procedure. To reduce the cyber security threats in the smart grid field, some researchers have presented security-related procedures for diverse reasons. The economic analysis of dynamic charging suggests that this technology could have significant cost savings for governments, fleet operators, and individual electric vehicle owners. By reducing the need for public charging infrastructure and enabling the electrification of previously impractical routes, dynamic charging could accelerate the adoption of electric vehicles and reduce greenhouse gas emissions.

7. Conclusions

In this paper, dynamic charging is treated as a favorable technology that has the potential to address the issue of range anxiety in electric vehicles. The economic analysis suggests that this technology could have significant cost savings for various stakeholders. The authors spoke about several computational as well as communication protocols and how they are used in the EV field. The emphasis lies on using EV industry standards and protocols in a variety of situations, including allowing charging periods, paying, running the charge depot, controlling the grid, and advanced charging use cases. For effective data transmission and security, V2X networking uses a variety of wireless connectivity protocols, including BLE, Zigbee, Lora, and Wi-Fi. In the article, use cases for communication technologies within the IoEV area were covered. To forecast charging behavior and locate charging stations in the best possible locations, computational methods like neural networks and ML are deployed. In addition to the aforementioned two use cases, ML algorithms may track the driver's behaviors and battery state. The use of big data technologies for the data obtained in the EV sector is also covered in the study. To help authors and researchers identify gaps in the EV study area and effectively perform their study, the authors have undertaken a thorough literature review on communication and computational technologies. For effective V2V, V2I, and V2P communication, a variety of standards and protocols are accessible. Deep learning and machine learning may be used to make decisions and predictive analytics to manage EV charging. For secure and transparent operations, energy trading platforms for EVs can leverage blockchain technology. In order to create frameworks, structures, and regulations for improved future prospects, the EV sector may employ each of the technologies and communication protocols stated above. Further research is needed to explore the economic implications of dynamic charging in different contexts and to identify any potential barriers to its widespread adoption.

Author Contributions: All the authors contributed equally to the manuscript preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Council of Scientific & Industrial Research (CSIR), India, under EMR II research scheme 22/0901/23/EMR-II. This research was also supported by the SGS grant from VSB—Technical University of Ostrava under grant number SP2024/018.

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

References

1. Venkatesan, R.; Savio, A.D.; Balaji, C.; Narayanamoorthi, R.; Kotb, H.; ELrashidi, A.; Nureldeen, W. A Comprehensive Review on Efficiency Enhancement of Wireless Charging System for the Electric Vehicles Applications. *IEEE Access* **2024**, *12*, 46967–46994. [[CrossRef](#)]
2. ElGhanam, E.; Sharf, H.; Odeh, Y.; Hassan, M.S.; Osman, A.H. On the Coordination of Charging Demand of Electric Vehicles in a Network of Dynamic Wireless Charging Systems. *IEEE Access* **2022**, *10*, 62879–62892. [[CrossRef](#)]
3. Zhang, X.; Yuan, Z.; Yang, Q.; Li, Y.; Zhu, J.; Li, Y. Coil Design and Efficiency Analysis for Dynamic Wireless Charging System for Electric Vehicles. *IEEE Trans. Magn.* **2016**, *52*, 8700404. [[CrossRef](#)]
4. Hamouid, K.; Adi, K. Privacy-aware Authentication Scheme for Electric Vehicle In-motion Wireless Charging. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 16–18 June 2020; pp. 1–6. [[CrossRef](#)]
5. Nguyen, T.-V.; Sun, H.; Wang, H.; Hu, R.Q. Authentication and PHY-Security Schemes for Electric Vehicle Dynamic Wireless Charging. *IEEE Trans. Veh. Technol.* **2024**, *73*, 1698–1712. [[CrossRef](#)]
6. Bianchi, T.; Asokraj, S.; Brighente, A.; Conti, M.; Poovendran, R. QEVSEC: Quick Electric Vehicle SECure Charging via Dynamic Wireless Power Transfer. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; pp. 1–6. [[CrossRef](#)]
7. Sikdar, S.; Damle, M. IoT Solutions for Electric Vehicles (EV) Charging Stations: A Driving Force Towards EV Mass Adoption. In Proceedings of the 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 18–19 November 2022; pp. 114–120. [[CrossRef](#)]
8. Hongwei, M.; Meng, Z.; Xu, F.; Xia, W. Study on coordinated charging control algorithm for plug-in electric vehicle based on energy internet. In Proceedings of the 2017 China International Electrical and Energy Conference (CIEEC), Beijing, China, 25–27 October 2017; pp. 653–657. [[CrossRef](#)]

9. Kadav, P.; Asher, Z.D. Improving the Range of Electric Vehicles. In Proceedings of the 2019 Electric Vehicles International Conference (EV), Bucharest, Romania, 3–4 October 2019; pp. 1–5. [[CrossRef](#)]
10. Yuan, K.; Sun, C.; Song, Y.; Xue, Z.; Wu, Z.; Gao, S.; Xu, J. Electric vehicle smart charging network under the energy internet framework. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–5. [[CrossRef](#)]
11. Halba, K.; Griffor, E.; Kamongi, P.; Roth, T. Using Statistical Methods and Co-Simulation to Evaluate ADS-Equipped Vehicle Trustworthiness. In Proceedings of the 2019 Electric Vehicles International Conference (EV), Bucharest, Romania, 3–4 October 2019; pp. 1–5. [[CrossRef](#)]
12. Wang, D.; Shi, Q.; Kong, W.; Dai, H. Research on the Development of Electric Vehicles and Vehicle to Grid. In Proceedings of the 2023 4th International Conference on Advanced Electrical and Energy Systems (AEES), Shanghai, China, 27–29 October 2023; pp. 614–619. [[CrossRef](#)]
13. Drosu, A.; Suci, G.; Scheianu, A.; Petre, I. An Analysis of Hybrid/Electric Vehicle Monitoring Systems and Parameters. In Proceedings of the 2019 Electric Vehicles International Conference (EV), Bucharest, Romania, 3–4 October 2019; pp. 1–5. [[CrossRef](#)]
14. Shaikh, P.W.; Mouftah, H.T. Connected and Autonomous Electric Vehicles Charging Reservation and Trip Planning System. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, 28 June–2 July 2021; pp. 1135–1140. [[CrossRef](#)]
15. Kaššaj, M.; Peráček, T. Synergies and Potential of Industry 4.0 and Automated Vehicles in Smart City Infrastructure. *Appl. Sci.* **2024**, *14*, 3575. [[CrossRef](#)]
16. Funta, R. Automated Driving and Data Protection: Some Remarks on Fundamental Rights and Privacy. *Crit. Law* **2021**, *13*, 106–118. [[CrossRef](#)]
17. Perișoară, L.A.; Dănișor, C.; Săcăleanu, D.I. Analysis of Mobile Communications Services for Internet of Things in Romania. In Proceedings of the 2022 23rd International Carpathian Control Conference (ICCC), Sinaia, Romania, 29 May–1 June 2022; pp. 198–202. [[CrossRef](#)]
18. Li, G.; Liu, P.; Wang, Z.; Zhang, Z.; Yan, Z.; Wang, S. An Overview of Cloud-Based Electric Vehicle Safety Service Platform Functions and A Case Study. In Proceedings of the 2021 6th International Conference on Transportation Information and Safety (ICTIS), Wuhan, China, 22–24 October 2021; pp. 1476–1481. [[CrossRef](#)]
19. Luo, L.; Feng, J.; Yu, H.; Sun, G. Blockchain-Enabled Two-Way Auction Mechanism for Electricity Trading in Internet of Electric Vehicles. *IEEE Internet Things J.* **2022**, *9*, 8105–8118. [[CrossRef](#)]
20. Yu, H.; Deng, J.; Wang, Z.; Wang, S. Research on Efficiency Interval Distribution of Permanent Magnet Synchronous Motor for Electric Vehicle Based on Operation Data Statistics. In Proceedings of the 2020 IEEE 29th International Symposium on Industrial Electronics (ISIE), Delft, Netherlands, 17–19 June 2020; pp. 362–367. [[CrossRef](#)]
21. Yang, Y.; Zhang, B.; Wang, W.; Wang, M.; Peng, X. Development Pathway and Practices for Integration of Electric Vehicles and Internet of Energy. In Proceedings of the 2020 IEEE Sustainable Power and Energy Conference (iSPEC), Chengdu, China, 23–25 November 2020; pp. 2128–2134. [[CrossRef](#)]
22. Muralidharan, M.; Karneswaran, S.G.; Elizabeth, E. Dynamic Charging Lane for Authenticated Electric Vehicles. In Proceedings of the 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 22–23 February 2024; pp. 1–5. [[CrossRef](#)]
23. Babu, P.R.; Reddy, A.G.; Palaniswamy, B.; Kommuri, S.K. EV-Auth: Lightweight Authentication Protocol Suite for Dynamic Charging System of Electric Vehicles with Seamless Handover. *IEEE Trans. Intell. Veh.* **2022**, *7*, 734–747. [[CrossRef](#)]
24. Babu, P.R.; Reddy, A.G.; Palaniswamy, B.; Das, A.K. EV-PUF: Lightweight Security Protocol for Dynamic Charging System of Electric Vehicles Using Physical Unclonable Functions. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3791–3807. [[CrossRef](#)]
25. Abouyoussef, M.; Ismail, M. Blockchain-Based Privacy-Preserving Networking Strategy for Dynamic Wireless Charging of EVs. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1203–1215. [[CrossRef](#)]
26. Massmi, K.; Hamouid, K.; Adi, K. Secure Electric Vehicle Dynamic Charging Based on Smart Contracts. In Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 23–26 October 2023; pp. 1–6. [[CrossRef](#)]
27. Pazos-Revilla, M.; Alsharif, A.; Gunukula, S.; Guo, T.N.; Mahmoud, M.; Shen, X. Secure and Privacy-Preserving Physical-Layer-Assisted Scheme for EV Dynamic Charging System. *IEEE Trans. Veh. Technol.* **2018**, *67*, 3304–3318. [[CrossRef](#)]
28. Alshaeri, A.; Younis, M. Lightweight Authentication and Authorization Protocol for Dynamic Charging of Electric Vehicles. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 550–556. [[CrossRef](#)]
29. Alshaeri, A.; Younis, M. A Blockchain-based Energy Trading Scheme for Dynamic Charging of Electric Vehicles. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6. [[CrossRef](#)]
30. Li, H.; Dán, G.; Nahrstedt, K. Portunes+: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging. *IEEE Trans. Smart Grid* **2017**, *8*, 2305–2313. [[CrossRef](#)]
31. Guo, T.; Mahmoud, M. Performance Analysis of Physical-Layer-Based Authentication for Electric Vehicle Dynamic Charging. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–7. [[CrossRef](#)]

32. Li, H.; Dan, G.; Nahrstedt, K. Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 920–925. [[CrossRef](#)]
33. Li, H.; Dán, G.; Nahrstedt, K. FADEC: Fast authentication for dynamic electric vehicle charging. In Proceedings of the 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 369–370. [[CrossRef](#)]
34. Gunukula, S.; Sherif, A.B.T.; Pazos-Revilla, M.; Ausby, B.; Mahmoud, M.; Shen, X.S. Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6. [[CrossRef](#)]
35. Razmjouei, P.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Jin, T.; Su, W. DAG-Based Smart Contract for Dynamic 6G Wireless EVs Charging System. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1459–1467. [[CrossRef](#)]
36. Li, H.; Dán, G.; Nahrstedt, K. Proactive key dissemination-based fast authentication for in-motion inductive EV charging. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 795–801. [[CrossRef](#)]
37. Almarshoodi, A.; Keenan, J.; Campbell, I.; Hassan, T.; Ibrahim, M.I.; Fouda, M.M. Security and Privacy Preservation for Future Vehicular Transportation Systems: A Survey. In Proceedings of the 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 8–9 April 2023; pp. 728–734. [[CrossRef](#)]
38. Fraiji, Y.; Azzouz, L.B.; Trojet, W.; Saidane, L.A.; Hoblos, G. Adaptive Security for the Intra-Electric Vehicular Wireless Networks. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1215–1220. [[CrossRef](#)]
39. Iqbal, A.; Rajasekaran, A.S.; Nikhil, G.S.; Azees, M. A Secure and Decentralized Blockchain Based EV Energy Trading Model Using Smart Contract in V2G Network. *IEEE Access* **2021**, *9*, 75761–75777. [[CrossRef](#)]
40. Yi, P.; Zhu, T.; Jiang, B.; Jin, R.; Wang, B. Deploying Energy Routers in an Energy Internet Based on Electric Vehicles. *IEEE Trans. Veh. Technol.* **2016**, *65*, 4714–4725. [[CrossRef](#)]
41. Qin, J.; Sun, X.; Wang, J.; Li, X.; Yin, L.; Zhang, R. Data-Driven Robust Day-Ahead Optimal Dispatch of Distribution Network Considering the Electric Vehicle. In Proceedings of the 2021 3rd International Conference on Smart Power & Internet Energy Systems (SPIES), Shanghai, China, 25–28 September 2021; pp. 322–327. [[CrossRef](#)]
42. Jia, Y.; Li, X.; Sang, L.; Wang, K. Research on Constant Voltage Output Optimization Method for EV Dynamic Wireless Charging System. In Proceedings of the 2020 8th International Conference on Power Electronics Systems and Applications (PESA), Hong Kong, China, 7–10 December 2020; pp. 1–4. [[CrossRef](#)]
43. Chowdary, K.V.V.S.R.; Kumar, K.; Behera, R.K.; Banerjee, S.; Kumar, R.R. Load Independent Characteristics of Dynamic Wireless Charging System Through Higher Order Compensation. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020; pp. 1–6. [[CrossRef](#)]
44. Prasad, K.K.; Agarwal, V. A Novel Frequency Modulation Technique to Minimize the Start-Up Transients in Dynamic Wireless Charging Systems for Electric Vehicles. In Proceedings of the 2022 Wireless Power Week (WPW), Bordeaux, France, 5–8 July 2022; pp. 834–838. [[CrossRef](#)]
45. Zavrel, M.; Kindl, V.; Tyrpekl, M. Dynamic Wireless Charging Using LCC-S Compensation Topology in Low and Medium Power Applications. In Proceedings of the 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE), Helsinki, Finland, 19–21 June 2023; pp. 1–6. [[CrossRef](#)]
46. Chowdary, K.V.V.S.R.; Kumar, K.; Nayak, B.; Mali, V. Decoding the Magnetic Coupler Characteristics for the Implementation of Dynamic Wireless Charging Scheme for Electric Vehicles. In Proceedings of the 2023 IEEE 3rd International Conference on Smart Technologies for Power, Energy and Control (STPEC), Bhubaneswar, India, 10–13 December 2023; pp. 1–6. [[CrossRef](#)]
47. Chowdary, K.V.V.S.R.; Kumar, K. Assessment of Dynamic Wireless Charging System with the Variation in Mutual Inductance. In Proceedings of the 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 24–26 November 2022; pp. 1–4. [[CrossRef](#)]
48. Yao, Y.; Du, L. Design of Intelligent Vehicle Based on Dynamic Wireless Charging. In Proceedings of the 2020 12th International Conference on Advanced Computational Intelligence (ICACI), Dali, China, 14–16 August 2020; pp. 402–407. [[CrossRef](#)]
49. Odeh, Y.S.; Elkahout, I.S.; Naeimi, P.V.; ElGhanam, E.A.; Hassan, M.S.; Osman, A.H. Planning and Allocation of Dynamic Wireless Charging Infrastructure for Electric Vehicles. In Proceedings of the 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE), Alanya, Turkey, 29–31 March 2022; pp. 306–310. [[CrossRef](#)]
50. Openshaw, S.; Etta, D.; Maji, S.; Ruan, T.; Afridi, K.K. Investigation of Commercial Viability and Public Perception of Electrified Roadways with Dynamic Wireless Charging. In Proceedings of the 2023 IEEE Wireless Power Technology Conference and Expo (WPTCE), San Diego, CA, USA, 4–8 June 2023; pp. 1–6. [[CrossRef](#)]
51. Jeong, S.; Jang, Y.J.; Kum, D. Economic Analysis of the Dynamic Charging Electric Vehicle. *IEEE Trans. Power Electron.* **2015**, *30*, 6368–6377. [[CrossRef](#)]

52. García-Vázquez, C.A.; Llorens-Iborra, F.; Fernández-Ramírez, L.M.; Sánchez-Sainz, H.; Jurado, F. Evaluating Dynamic Wireless Charging of electric vehicles moving along a stretch of highway. In Proceedings of the 2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), Capri, Italy, 22–24 June 2016; pp. 61–66. [[CrossRef](#)]
53. Haddad, D.; Arellano, P.; Bernicke, D.; Castilho, M.; Gilley, B.; Lagpacan, Z.; Maxey, C.; Pilaszewicz, A.; Young, W.; Aliprantis, D. Economic Feasibility of Dynamic Wireless Power Transfer Lanes in Indiana Freight Corridors. In Proceedings of the 2022 IEEE Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 10–11 March 2022; pp. 1–8. [[CrossRef](#)]
54. Alattab, A.A.; Irshad, R.R.; Yahya, A.A.; Al-Awady, A.A. Privacy Protected Preservation of Electric Vehicles' Data in Cloud Computing Using Secure Data Access Control. *Energies* **2022**, *15*, 8085. [[CrossRef](#)]
55. Tappeta, V.S.R.; Appasani, B.; Patnaik, S.; Ustun, T.S. A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles. *Energies* **2022**, *15*, 6580. [[CrossRef](#)]
56. Piedel, E.; Lauth, E.; Grahle, A.; Göhlich, D. Review and Evaluation of Automated Charging Technologies for Heavy-Duty Vehicles. *World Electr. Veh. J.* **2024**, *15*, 235. [[CrossRef](#)]
57. Kulkarni, G.A.; Joshi, R.D. Electric vehicle charging station integration with IOT enabled device. In Proceedings of the 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), Jaipur, India, 1–2 December 2021; pp. 1–6. [[CrossRef](#)]
58. Zhang, X.; Yang, Y.; Su, S. Study on Electric Vehicle Sharing and Leasing Business Model for Group Users based on Blockchain. In Proceedings of the 2020 IEEE Sustainable Power and Energy Conference (iSPEC), Chengdu, China, 23–25 November 2020; pp. 2628–2633. [[CrossRef](#)]
59. Durga, C.R.; Karthik, J.; Dakshayani, R.; Manikanta, S. A Novel Approach for Smart Battery Monitoring System in Electric Vehicles using Internet of Things. In Proceedings of the 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 5–7 January 2023; pp. 870–874. [[CrossRef](#)]
60. Zhang, Y.; Xu, H. Reconfigurable-Intelligent-Surface-Enhanced Dynamic Resource Allocation for the Social Internet of Electric Vehicle Charging Networks with Causal-Structure-Based Reinforcement Learning. *Future Internet* **2024**, *16*, 165. [[CrossRef](#)]
61. Shanmugam, Y.; Rajamanickam, N.; Alroobaea, R.; Afandi, A. Driving towards Sustainability: Wireless Charging of Low-Speed Vehicles with PDM-Based Active Bridge Rectifiers. *Sustainability* **2024**, *16*, 3810. [[CrossRef](#)]
62. Ahn, S.; Jung, H.; Park, K.-W. LazyFrog: Advancing Security and Efficiency in Commercial Wireless Charging with Adaptive Frequency Hopping. *Sensors* **2024**, *24*, 2571. [[CrossRef](#)] [[PubMed](#)]
63. Li, J.; Deng, Z.; Feng, Y.; Liu, N. Deep-Reinforcement-Learning-Based Joint Energy Replenishment and Data Collection Scheme for WRSN. *Sensors* **2024**, *24*, 2386. [[CrossRef](#)]
64. Behnamfar, M.; Stevenson, A.; Tariq, M.; Sarwat, A. Vehicle Position Detection Based on Machine Learning Algorithms in Dynamic Wireless Charging. *Sensors* **2024**, *24*, 2346. [[CrossRef](#)]
65. Jung, S. Precision Landing of Unmanned Aerial Vehicle under Wind Disturbance Using Derivative Sliding Mode Nonlinear Disturbance Observer-Based Control Method. *Aerospace* **2024**, *11*, 265. [[CrossRef](#)]
66. Zhu, X.; Fan, H.; Zhang, S.; Du, J. Stochastic Optimization of an Electric Bus Dynamic Wireless Charging System. *World Electr. Veh. J.* **2024**, *15*, 137. [[CrossRef](#)]
67. Rabih, M.; Takruri, M.; Al-Hattab, M.; Alnuaimi, A.A.; Bin Thaleth, M.R. Wireless Charging for Electric Vehicles: A Survey and Comprehensive Guide. *World Electr. Veh. J.* **2024**, *15*, 118. [[CrossRef](#)]
68. Wang, J.; Wang, S.; Wen, K.; Weng, B.; Zhou, X.; Chen, K. An ECC-Based Authentication Protocol for Dynamic Charging System of Electric Vehicles. *Electronics* **2024**, *13*, 1109. [[CrossRef](#)]
69. Iqbal, S.; Alshammari, N.F.; Shouran, M.; Massoud, J. Smart and Sustainable Wireless Electric Vehicle Charging Strategy with Renewable Energy and Internet of Things Integration. *Sustainability* **2024**, *16*, 2487. [[CrossRef](#)]
70. Sabban, A. Novel Meta-Fractal Wearable Sensors and Antennas for Medical, Communication, 5G, and IoT Applications. *Fractal Fract.* **2024**, *8*, 100. [[CrossRef](#)]
71. Bertoluzzo, M.; Di Barba, P.; Forzan, M.; Mognaschi, M.E.; Sieni, E. A Deep Learning Approach to Improve the Control of Dynamic Wireless Power Transfer Systems. *Energies* **2023**, *16*, 7865. [[CrossRef](#)]
72. Quadir, N.; Alawar, F.S.; Albasha, L.; Mir, H. Linear-in-dB Logarithmic Signal Strength Sensor Circuit for Wireless Power Transfer Receivers. *Energies* **2023**, *16*, 7612. [[CrossRef](#)]
73. Bozhi, Mohamed, M.; Gilani, V.N.M.; Amjad, A.; Majid, M.S.; Yahya, K.; Salem, M. A Review of Wireless Pavement System Based on the Inductive Power Transfer in Electric Vehicles. *Sustainability* **2023**, *15*, 14893. [[CrossRef](#)]
74. Liang, M.; El Khamlichi Drissi, K.; Pasquier, C. Self- and Mutual-Inductance Cross-Validation of Multi-Turn, Multi-Layer Square Coils for Dynamic Wireless Charging of Electric Vehicles. *Energies* **2023**, *16*, 7033. [[CrossRef](#)]
75. Chowdary, K.V.V.S.R.; Kumar, K.; Nayak, B.; Kumar, A.; Bertoluzzo, M. Dynamic Wireless Charging Performance Enhancement for Electric Vehicles: Mutual Inductance, Power Transfer Capability, and Efficiency. *Vehicles* **2023**, *5*, 1313–1327. [[CrossRef](#)]
76. Allama, O.; Habaebi, M.H.; Khan, S.; Islam, M.R.; Alghaihab, A. Simulation and Control Design of a Midrange WPT Charging System for In-Flight Drones. *Energies* **2023**, *16*, 5746. [[CrossRef](#)]
77. Bensetti, M.; Kadem, K.; Pei, Y.; Le Bihan, Y.; Labouré, E.; Pichon, L. Parametric Optimization of Ferrite Structure Used for Dynamic Wireless Power Transfer for 3 kW Electric Vehicle. *Energies* **2023**, *16*, 5439. [[CrossRef](#)]

78. Zhang, B.; Gong, C.; Wang, Y.; Ma, L.; Zhang, D.; Xia, S. Research on the Collaborative Optimization of the Power Distribution Network and Traffic Network Based on Dynamic Traffic Allocation. *Energies* **2023**, *16*, 5259. [[CrossRef](#)]
79. Bourzik, M.; Elbaz, H.; Bouleft, Y.; Alaoui, A.E.H. Round-Trip Wireless Charging Infrastructure for Heterogeneous Electric Vehicles on Highways: Modelling and Optimization. *World Electr. Veh. J.* **2023**, *14*, 160. [[CrossRef](#)]
80. Wang, W.; Fan, S.; Wang, Z.; Yao, X.; Mu, K. Optimal Driving Model for Connected and Automated Electric Freight Vehicles in a Wireless Charging Scenario at Signalised Intersections. *Appl. Sci.* **2023**, *13*, 6286. [[CrossRef](#)]
81. Xiong, W.; Liu, J.; Chen, J.; Hu, D. Detection of Secondary Side Position for Segmented Dynamic Wireless Charging Systems Based on Primary Phase Angle Sensing. *Electronics* **2023**, *12*, 2148. [[CrossRef](#)]
82. Tang, Q.; Li, D.; Zhang, Y.; Chen, X. Dynamic Path-Planning and Charging Optimization for Autonomous Electric Vehicles in Transportation Networks. *Appl. Sci.* **2023**, *13*, 5476. [[CrossRef](#)]
83. Xu, F.; Wei, S.; Yuan, D.; Li, J. Review on Key Technologies and Development of Magnetic Coupling Resonant-Dynamic Wireless Power Transfer for Unmanned Ground Vehicles. *Electronics* **2023**, *12*, 1506. [[CrossRef](#)]
84. Dimitriadou, K.; Rigogiannis, N.; Fountoukidis, S.; Kotarela, F.; Kyritsis, A.; Papanikolaou, N. Current Trends in Electric Vehicle Charging Infrastructure; Opportunities and Challenges in Wireless Charging Integration. *Energies* **2023**, *16*, 2057. [[CrossRef](#)]
85. Wang, Y.; Gong, L.; Bao, B.; Pan, J.; Feng, Q.; Xu, R. Conceptual Design and Preliminary Verification of Distributed Wireless System of Weigh-in-Motion. *Appl. Sci.* **2023**, *13*, 2467. [[CrossRef](#)]
86. Hakemi, A.; Jovanovic, D.; Vilathgamuwa, M.; Walker, G.R. Robust Maximum Efficiency Tracking Control of Wirelessly Powered Directly Supplied Heart Pumps. *Energies* **2023**, *16*, 1517. [[CrossRef](#)]
87. Ganchev, I.; O'Droma, M. Outsourcing Authentication, Authorization and Accounting, and Charging and Billing Services to Trusted Third Parties for Future Consumer-Oriented Wireless Communications. *Electronics* **2023**, *12*, 558. [[CrossRef](#)]
88. Park, J.-H.; Joe, I.-W. Federated Learning-Based Prediction of Energy Consumption from Blockchain-Based Black Box Data for Electric Vehicles. *Appl. Sci.* **2024**, *14*, 5494. [[CrossRef](#)]
89. Xu, Y.; Alderete Peralta, A.; Balta-Ozkan, N. Vehicle-to-Vehicle Energy Trading Framework: A Systematic Literature Review. *Sustainability* **2024**, *16*, 5020. [[CrossRef](#)]
90. Kim, M.; Park, K.; Park, Y. A Reliable and Privacy-Preserving Vehicular Energy Trading Scheme Using Decentralized Identifiers. *Mathematics* **2024**, *12*, 1450. [[CrossRef](#)]
91. Khan, S.; Amin, U.; Abu-Siada, A. P2P Energy Trading of EVs Using Blockchain Technology in Centralized and Decentralized Networks: A Review. *Energies* **2024**, *17*, 2135. [[CrossRef](#)]
92. Miao, Q.; Ren, T.; Dong, J.; Chen, Y.; Xu, W. A 3C Authentication: A Cross-Domain, Certificateless, and Consortium-Blockchain-Based Authentication Method for Vehicle-to-Grid Networks in a Smart Grid. *Symmetry* **2024**, *16*, 336. [[CrossRef](#)]
93. Stetter, D.; Höpfer, T.; Schmid, M.; Sturz, I.; Falkenberger, S.; Knoll, N. BANULA—A Novel DLT-Based Approach for EV Charging with High Level of User Comfort and Role-Specific Data Transparency for All Parties Involved. *World Electr. Veh. J.* **2024**, *15*, 79. [[CrossRef](#)]
94. Chougule, S.B.; Chaudhari, B.S.; Ghorpade, S.N.; Zennaro, M. Exploring Computing Paradigms for Electric Vehicles: From Cloud to Edge Intelligence, Challenges and Future Directions. *World Electr. Veh. J.* **2024**, *15*, 39. [[CrossRef](#)]
95. Samadi, M.; Ruj, S.; Schriemer, H.; Erol-Kantarci, M. Secure and Robust Demand Response Using Stackelberg Game Model and Energy Blockchain. *Sensors* **2023**, *23*, 8352. [[CrossRef](#)]
96. Singh, M.; Ahmed, S.; Sharma, S.; Singh, S.; Yoon, B. BSEMS—A Blockchain-Based Smart Energy Measurement System. *Sensors* **2023**, *23*, 8086. [[CrossRef](#)]
97. Wang, X.; Wei, J.; Wen, F.; Wang, K. A Trading Mode Based on the Management of Residual Electric Energy in Electric Vehicles. *Energies* **2023**, *16*, 6317. [[CrossRef](#)]
98. Aldweesh, A. A Blockchain-Based Data Authentication Algorithm for Secure Information Sharing in Internet of Vehicles. *World Electr. Veh. J.* **2023**, *14*, 223. [[CrossRef](#)]
99. Cui, D.; He, J.; Cheng, X.; Liu, Z. Electric Vehicle Charging Transaction Model Based on Alliance Blockchain. *World Electr. Veh. J.* **2023**, *14*, 192. [[CrossRef](#)]
100. Naseri, F.; Kazemi, Z.; Larsen, P.G.; Arefi, M.M.; Schaltz, E. Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects. *Batteries* **2023**, *9*, 382. [[CrossRef](#)]
101. Mousavi, P.; Ghazizadeh, M.S.; Vahidinasab, V. A Decentralized Blockchain-Based Energy Market for Citizen Energy Communities. *Inventions* **2023**, *8*, 86. [[CrossRef](#)]
102. Cabrera-Gutiérrez, A.J.; Castillo, E.; Escobar-Molero, A.; Cruz-Cozar, J.; Morales, D.P.; Parrilla, L. Blockchain-Based Services Implemented in a Microservices Architecture Using a Trusted Platform Module Applied to Electric Vehicle Charging Stations. *Energies* **2023**, *16*, 4285. [[CrossRef](#)]
103. Cavalcante, I.; Júnior, J.; Manzolli, J.A.; Almeida, L.; Pungo, M.; Guzman, C.P.; Morais, H. Electric Vehicles Charging Using Photovoltaic Energy Surplus: A Framework Based on Blockchain. *Energies* **2023**, *16*, 2694. [[CrossRef](#)]
104. Waseem, M.; Adnan Khan, M.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. [[CrossRef](#)]
105. Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and Machine Learning for Future Smart Grids: A Review. *Energies* **2023**, *16*, 528. [[CrossRef](#)]

106. Zondervan, N.A.; Tolentino-Zondervan, F.; Moeke, D. Logistics Trends and Innovations in Response to COVID-19 Pandemic: An Analysis Using Text Mining. *Processes* **2022**, *10*, 2667. [[CrossRef](#)]
107. Espina-Romero, L.; Guerrero-Alcedo, J.; Noroño Sánchez, J.G.; Ochoa-Díaz, A. What Are the Topics That Business Ecosystems Navigate? Updating of Scientific Activity and Future Research Agenda. *Sustainability* **2022**, *14*, 16224. [[CrossRef](#)]
108. Guo, W.; Chang, Z.; Su, Y.; Guo, X.; Hämäläinen, T.; Li, J.; Li, Y. Reputation-Based Blockchain for Spatial Crowdsourcing in Vehicular Networks. *Appl. Sci.* **2022**, *12*, 11049. [[CrossRef](#)]
109. Teimoori, Z.; Yassine, A. A Review on Intelligent Energy Management Systems for Future Electric Vehicle Transportation. *Sustainability* **2022**, *14*, 14100. [[CrossRef](#)]
110. Biegańska, M. IoT-Based Decentralized Energy Systems. *Energies* **2022**, *15*, 7830. [[CrossRef](#)]
111. Seven, S.; Yoldas, Y.; Soran, A.; Yalcin Alkan, G.; Jung, J.; Ustun, T.S.; Onen, A. Energy Trading on a Peer-to-Peer Basis between Virtual Power Plants Using Decentralized Finance Instruments. *Sustainability* **2022**, *14*, 13286. [[CrossRef](#)]
112. Enescu, F.M.; Birleanu, F.G.; Raboaca, M.S.; Bizon, N.; Thounthong, P. A Review of the Public Transport Services Based on the Blockchain Technology. *Sustainability* **2022**, *14*, 13027. [[CrossRef](#)]
113. Kakkar, R.; Gupta, R.; Agrawal, S.; Tanwar, S.; Altameem, A.; Altameem, T.; Sharma, R.; Turcanu, F.-E.; Raboaca, M.S. Blockchain and IoT-Driven Optimized Consensus Mechanism for Electric Vehicle Scheduling at Charging Stations. *Sustainability* **2022**, *14*, 12800. [[CrossRef](#)]
114. Trivedi, M.; Kakkar, R.; Gupta, R.; Agrawal, S.; Tanwar, S.; Niculescu, V.-C.; Raboaca, M.S.; Alqahtani, F.; Saad, A.; Tolba, A. Blockchain and Deep Learning-Based Fault Detection Framework for Electric Vehicles. *Mathematics* **2022**, *10*, 3626. [[CrossRef](#)]
115. Roozbehani, M.M.; Heydarian-Forushani, E.; Hasanzadeh, S.; Elghali, S.B. Virtual Power Plant Operational Strategies: Models, Markets, Optimization, Challenges, and Opportunities. *Sustainability* **2022**, *14*, 12486. [[CrossRef](#)]
116. Khan, H.; Masood, T. Impact of Blockchain Technology on Smart Grids. *Energies* **2022**, *15*, 7189. [[CrossRef](#)]
117. Kaushal, R.K.; Agal, S.; Singh, N.B.R.; Singh, P.P. SVM Modeling Simulation to Evaluate the Electric Vehicle Transmitting Points. In Proceedings of the 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 25–26 May 2023; pp. 1–7. [[CrossRef](#)]
118. Ashfaq, T.; Khalid, M.I.; Ali, G.; Affendi, M.E.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Yahaya, A.S.; Khalid, R.; Mateen, A. An Efficient and Secure Energy Trading Approach with Machine Learning Technique and Consortium Blockchain. *Sensors* **2022**, *22*, 7263. [[CrossRef](#)]
119. Xue, F.; Chang, K.; Li, W.; Wang, Q.; Zhao, H.; Zhang, H.; Ni, Y.; Xia, W. Blockchain Smart Contract-Enabled Secure Energy Trading for Electric Vehicles. *Energies* **2022**, *15*, 6733. [[CrossRef](#)]
120. Wang, N.; Garg, A.; Su, S.; Mou, J.; Gao, L.; Li, W. Echelon Utilization of Retired Power Lithium-Ion Batteries: Challenges and Prospects. *Batteries* **2022**, *8*, 96. [[CrossRef](#)]
121. Ghobadpour, A.; Monsalve, G.; Cardenas, A.; Mousazadeh, H. Off-Road Electric Vehicles and Autonomous Robots in Agricultural Sector: Trends, Challenges, and Opportunities. *Vehicles* **2022**, *4*, 843–864. [[CrossRef](#)]
122. Kakkar, R.; Gupta, R.; Agrawal, S.; Bhattacharya, P.; Tanwar, S.; Raboaca, M.S.; Alqahtani, F.; Tolba, A. Blockchain and Double Auction-Based Trustful EVs Energy Trading Scheme for Optimum Pricing. *Mathematics* **2022**, *10*, 2748. [[CrossRef](#)]
123. Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Birleanu, F.G.; Takorabet, N.; Thounthong, P.; Bizon, N. Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions. *Sustainability* **2022**, *14*, 8801. [[CrossRef](#)]
124. Miao, J. Design of a Data Security Access Control Algorithm for the Electric Vehicle Internet of Vehicles Based on Blockchain Technology. *World Electr. Veh. J.* **2022**, *13*, 111. [[CrossRef](#)]
125. Juszczak, O.; Shahzad, K. Blockchain Technology for Renewable Energy: Principles, Applications and Prospects. *Energies* **2022**, *15*, 4603. [[CrossRef](#)]
126. Xiao, J.; Hou, W. Cost Estimation Process of Green Energy Production and Consumption Using Probability Learning Approach. *Sustainability* **2022**, *14*, 7091. [[CrossRef](#)]
127. Kapassa, E.; Themistocleous, M. Blockchain Technology Applied in IoV Demand Response Management: A Systematic Literature Review. *Future Internet* **2022**, *14*, 136. [[CrossRef](#)]
128. Rimal, B.P.; Kong, C.; Poudel, B.; Wang, Y.; Shahi, P. Smart Electric Vehicle Charging in the Era of Internet of Vehicles, Emerging Trends, and Open Issues. *Energies* **2022**, *15*, 1908. [[CrossRef](#)]
129. Kapassa, E.; Themistocleous, M.; Christodoulou, K.; Iosif, E. Blockchain Application in Internet of Vehicles: Challenges, Contributions and Current Limitations. *Future Internet* **2021**, *13*, 313. [[CrossRef](#)]
130. Santos, J.B.; Francisco, A.M.B.; Cabrita, C.; Monteiro, J.; Pacheco, A.; Cardoso, P.J.S. Development and Implementation of a Smart Charging System for Electric Vehicles Based on the ISO 15118 Standard. *Energies* **2024**, *17*, 3045. [[CrossRef](#)]
131. Uribe-Pérez, N.; Gonzalez-Garrido, A.; Gallarreta, A.; Justel, D.; González-Pérez, M.; González-Ramos, J.; Arrizabalaga, A.; Asensio, F.J.; Bidaguren, P. Communications and Data Science for the Success of Vehicle-to-Grid Technologies: Current State and Future Trends. *Electronics* **2024**, *13*, 1940. [[CrossRef](#)]
132. Kirchner, S.R. OCPP Interoperability: A Unified Future of Charging. *World Electr. Veh. J.* **2024**, *15*, 191. [[CrossRef](#)]
133. Boutsidiadis, E.; Pasialis, N.; Lettas, N.; Tsiamitros, D.; Stimoniaris, D. Distributed Generation Control Using Ripple Signaling and a Multiprotocol Communication Embedded Device. *Energies* **2023**, *16*, 7604. [[CrossRef](#)]

134. Zeinali, M.; Erdogan, N.; Bayram, I.S.; Thompson, J.S. Impact of Communication System Characteristics on Electric Vehicle Grid Integration: A Large-Scale Practical Assessment of the UK's Cellular Network for the Internet of Energy. *Electricity* **2023**, *4*, 309–319. [[CrossRef](#)]
135. Sánchez Díaz, C.A.; Díaz Lucio, A.S.; Salazar-Cabrera, R.; Pachón de la Cruz, Á.; Madrid Molina, J.M. Prototype of a System for Tracking Transit Service Based on IoV, ITS, and Machine Learning. *World Electr. Veh. J.* **2023**, *14*, 261. [[CrossRef](#)]
136. Park, S.; Lee, E.; Noh, Y.-H.; Choi, D.-H.; Yook, J.-g. Accurate Modeling of CCS Combo Type 1 Cable and Its Communication Performance Analysis for High-Speed EV-EVSE Charging System. *Energies* **2023**, *16*, 5947. [[CrossRef](#)]
137. Babangida, A.; Light Odazie, C.M.; Szemes, P.T. Optimal Control Design and Online Controller-Area-Network Bus Data Analysis for a Light Commercial Hybrid Electric Vehicle. *Mathematics* **2023**, *11*, 3436. [[CrossRef](#)]
138. Jeffrey, N.; Tan, Q.; Villar, J.R. A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electronics* **2023**, *12*, 3283. [[CrossRef](#)]
139. Dipon, W.; Gamboa, B.; Estrada, M.; Flynn, W.P.; Guo, R.; Bhalla, A. Self-Sustainable IoT-Based Remote Sensing Powered by Energy Harvesting Using Stacked Piezoelectric Transducer and Thermoelectric Generator. *Micromachines* **2023**, *14*, 1428. [[CrossRef](#)] [[PubMed](#)]
140. Rathje, P.; Poirot, V.; Landsiedel, O. STARC: Decentralized Coordination Primitive on Low-Power IoT Devices for Autonomous Intersection Management. *J. Sens. Actuator Netw.* **2023**, *12*, 56. [[CrossRef](#)]
141. Gwon, M.; Lee, K.; Park, J.; Kim, J. Establishment of Real-Time Simulation Test Environment for Electric Propulsion System of Unmanned Aerial Vehicle Using KDECAN Communication. *Electronics* **2023**, *12*, 3008. [[CrossRef](#)]
142. Alden, R.E.; Gong, H.; Rooney, T.; Branecky, B.; Ionel, D.M. Electric Water Heater Modeling for Large-Scale Distribution Power Systems Studies with Energy Storage CTA-2045 Based VPP and CVR. *Energies* **2023**, *16*, 4747. [[CrossRef](#)]
143. Kraemer, R.A.S.; Lodetti, P.Z.; Silva, A.C.d.; Cardoso, B.B.; Vicente, I.; Martins, M.A.I.; Simões, A.d.P.; Spader, N. Regulatory Challenges in the Electromobility Sector: An Analysis of Electric Buses in Brazil. *Energies* **2023**, *16*, 3510. [[CrossRef](#)]
144. Rautenberg, P.; Weber, P.; Degel, J.P.; Hähnlein, S.; Gauterin, F.; Koch, T.; Doppelbauer, M.; Gohl, M. Electrified Powertrain Development: Distributed Co-Simulation Protocol Extension for Coupled Test Bench Operations. *Appl. Sci.* **2023**, *13*, 2657. [[CrossRef](#)]
145. Alzahrani, A.; Wangikar, S.M.; Indragandhi, V.; Singh, R.R.; Subramaniaswamy, V. Design and Implementation of SAE J1939 and Modbus Communication Protocols for Electric Vehicle. *Machines* **2023**, *11*, 201. [[CrossRef](#)]
146. Anusha, T.; Pushpalatha, M. Efficient Communication Model for a Smart Parking System with Multiple Data Consumers. *Smart Cities* **2022**, *5*, 1536–1553. [[CrossRef](#)]
147. Almuhaideb, A.M.; Algothami, S.S. Efficient Privacy-Preserving and Secure Authentication for Electric-Vehicle-to-Electric-Vehicle-Charging System Based on ECQV. *J. Sens. Actuator Netw.* **2022**, *11*, 28. [[CrossRef](#)]
148. Basavaraj, D.; Tayeb, S. Towards a Lightweight Intrusion Detection Framework for In-Vehicle Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 6. [[CrossRef](#)]
149. Luciani, S.; Feraco, S.; Bonfitto, A.; Tonoli, A. Hardware-in-the-Loop Assessment of a Data-Driven State of Charge Estimation Method for Lithium-Ion Batteries in Hybrid Vehicles. *Electronics* **2021**, *10*, 2828. [[CrossRef](#)]
150. Chen, T.; Li, X. (Semi-)Automatically Parsing Private Protocols for In-Vehicle ECU Communications. *Entropy* **2021**, *23*, 1495. [[CrossRef](#)]
151. Habeeb, S.A.; Tostado-Véliz, M.; Hasanien, H.M.; Turky, R.A.; Meteab, W.K.; Jurado, F. DC Nanogrids for Integration of Demand Response and Electric Vehicle Charging Infrastructures: Appraisal, Optimal Scheduling and Analysis. *Electronics* **2021**, *10*, 2484. [[CrossRef](#)]
152. Tramacere, E.; Luciani, S.; Feraco, S.; Bonfitto, A.; Amati, N. Processor-in-the-Loop Architecture Design and Experimental Validation for an Autonomous Racing Vehicle. *Appl. Sci.* **2021**, *11*, 7225. [[CrossRef](#)]
153. Gehlot, A.; Alshamrani, S.S.; Singh, R.; Rashid, M.; Akram, S.V.; AlGhamdi, A.S.; Albogamy, F.R. Internet of Things and Long-Range-Based Smart Lampposts for Illuminating Smart Cities. *Sustainability* **2021**, *13*, 6398. [[CrossRef](#)]
154. Chamberlain, K.; Al-Majeed, S. Standardisation of UK Electric Vehicle Charging Protocol, Payment and Charge Point Connection. *World Electr. Veh. J.* **2021**, *12*, 63. [[CrossRef](#)]
155. Gaggero, G.B.; Marchese, M.; Moheddine, A.; Patrone, F. A Possible Smart Metering System Evolution for Rural and Remote Areas Employing Unmanned Aerial Vehicles and Internet of Things in Smart Grids. *Sensors* **2021**, *21*, 1627. [[CrossRef](#)]
156. Mlýnek, P.; Ruzs, M.; Beneš, L.; Sláček, J.; Musil, P. Possibilities of Broadband Power Line Communications for Smart Home and Smart Building Applications. *Sensors* **2021**, *21*, 240. [[CrossRef](#)]
157. Guerrero Alonso, J.I.; Personal, E.; García, S.; Parejo, A.; Rossi, M.; García, A.; Delfino, F.; Pérez, R.; León, C. Flexibility Services Based on OpenADR Protocol for DSO Level. *Sensors* **2020**, *20*, 6266. [[CrossRef](#)]
158. Kaveh, M.; Martín, D.; Mosavi, M.R. A Lightweight Authentication Scheme for V2G Communications: A PUF-Based Approach Ensuring Cyber/Physical Security and Identity/Location Privacy. *Electronics* **2020**, *9*, 1479. [[CrossRef](#)]
159. Kupzog, F.; Veichtlbauer, A.; Heinisch, A.; von Tüllenbur, F.; Langthaler, O.; Pache, U.; Jung, O.; Frank, R.; Dorfinger, P. The Impact of Virtualisation Techniques on Power System Control Networks. *Electronics* **2020**, *9*, 1433. [[CrossRef](#)]

-
160. El Hariri, M.; Youssef, T.; Saleh, M.; Faddel, S.; Habib, H.; Mohammed, O.A. A Framework for Analyzing and Testing Cyber-Physical Interactions for Smart Grid Applications. *Electronics* **2019**, *8*, 1455. [[CrossRef](#)]
 161. Park, J.; Kim, H.; Choi, J.-Y. Improving TCP Performance in Vehicle-To-Grid (V2G) Communication. *Electronics* **2019**, *8*, 1206. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.