Review

The Internet of Vehicles and Sustainability—Reflections on   
Environmental, Social, and Corporate Governance

Mariusz Kostrzewski 1,\*, Magdalena Marczewska 2 and Lorna Uden 3

|  |
| --- |
| **Citation:** Kostrzewski, M.; Marczewska, M.; Uden, L. The Internet of Vehicles and Sustainability—Reflections on Environmental,  Social, and Corporate Governance. *Energies* **2023**, *16*, x. https://doi.org/10.3390/xxxxx  Academic Editor(s):  Received: date  Revised: date  Accepted: date  Published: date    **Copyright:** © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/). |

1 Faculty of Transport, Warsaw University of Technology, Koszykowa 75, 00-662 Warsaw, Poland

2 Faculty of Management, University of Warsaw, 1/3 Szturmowa Street, 02-678 Warsaw, Poland;   
mmarczewska@wz.uw.edu.pl

3 School of Computing, Staffordshire University, College Road, Stoke-on-Trent, Staffordshire ST4 2DE, UK; l.uden@staffs.ac.uk

**\*** Correspondence: mariusz.kostrzewski@pw.edu.pl

**Abstract:** TheInternet of Vehicles (IoV) has generated great interest among researchers from different disciplines as it is multidisciplinary research. Sustainability for the IoV requires solutions from different perspectives, particularly in the context of environmental, social, and corporate governance. This review paper examines each of the mentioned perspectives of IoV research which were conducted among at least one of these three perspectives. On the one hand, this allows determining how widely research on the IoV system has been conducted. Moreover, it shows the directions of research on the IoV. On the other hand, it determines whether and how the IoV research is linked to each of the perspectives separately and analyses this link from a global perspective as well; i.e., it analyses the survey data in terms of the data’s relationship to all the perspectives as a group. As one of the research results, a conceptual model of IoV systems allocating the ESG perspectives was developed. The current research has shown that consideration of IoV systems in the context of these three perspectives (treated both individually and collectively) is still limited. A balanced approach towards these IoV systems is still required. Therefore, the paper consists of a survey of the current research related to the sustainability of the IoV from the three mentioned perspectives, aiming to give a balanced view of the importance of the three perspectives for IoV systems.

**Keywords:** Internet of Vehicles; IoV; environmental, social, and corporate governance; ESG; VANET; SIoV; road transport

1. Introduction

Maintaining the sustainability of transportation has always been a challenge. Global commitments to achieving sustainable development and environmental protection are gaining importance in transportation. New ideas and technologies in the transportation systems create opportunities ranging from improving the overall travel experience to improving transportation sustainability. The Internet of Vehicles (IoV) provides a group of potential solutions to help ensure more sustainable traveling. This group of potential solutions is related to, e.g., road traffic safety maintenance, the use of pollution-free vehicular systems, collisions, or accident prevention [1,2], social innovations for sustainable transport and infrastructure [3], and good governance in terms of IoV-related data protection, information privacy, and usage [4]. The IoV allows us to collect data and operate based on real-time predictions rather than on static data [5], which, used and managed wisely, may help in improving transportation sustainability.

Sustainability concerning the IoV should be analyzed and tackled under three contemporarily significant, underpinning perspectives: environmental, social, and corporate governance (concerning the concept of environmental, social, and corporate governance; acronym: ESG) [6,7]. ESG indicators are increasingly used for decision making by governments, markets, companies, investors, and other institutional entities [8–11]. Most empirical studies support the notion that ESG performance is positively related to company performance [6], supply chain relationships [12,13], and sustainability [14]. The multidimensional and holistic analysis of the IoV concept through the ESG prism will allow for the development of a conceptual model for sustainable IoV design. Thus, the goal of this conceptual paper is to gain insight into the possibility that the IoV will make the transport system more sustainable, considering ESG as the main framework for analysis. The contribution of the paper is threefold. Firstly, it contributes to building a better understanding of the IoV and related concepts. This understanding is expressed through an extensive literature review and synthesis. Secondly, it presents the IoV in relation to three different dimensions of sustainability—the environmental, social, and governance perspectives. Thirdly, it concludes with a conceptual model describing the dimensions of a sustainable IoV.

This paper follows a scoping review research method. This exploratory research method aims to map the literature on a given research subject or research area and enable the identification of major concepts and research gaps through systematic search, selection, and synthesis of existing knowledge [15–17].

This paper starts with explaining the IoV and related concepts, terms, and definitions. Then, it continues by exploring IoV design and applications within the ESG framework. The paper concludes with a conceptual model describing the dimensions of a sustainable IoV followed by conclusions together with research agendas and implications.

2. IoV and Related Concepts

The IoV is a distributed network that supports the use of data created by connected cars and vehicular ad hoc networks (VANETs); in a nutshell, it is where vehicles build and manage their social networks [18]. The IoV is sometimes called the Internet of Connected Vehicles (IoCV), as mentioned in [19], or the Vehicular Internet of Things (VIoT), as given in [18], or even the Social Internet of Vehicles (SIoV) [20]. The IoV originated from VANETs. The evolution of VANETs into the IoV was presented in [21]. As it was shortly defined in [22], the “VANET is a type of mobile ad hoc network (MANET) with road routes, which aim to provide traffic safety, improve traffic flow, and enhance the driving experiences.” In contrast, in [23] it is defined as “a type of Mobile Ad hoc NETwork (MANET), enables the communication between vehicles (V2V) and between vehicles and infrastructure (V2I) [24].” VANETs are considered a branch of MANETs characterized by the presence of moving vehicles with On-Board Units (OBUs), which enable connectivity with a network and allow passengers to use internet devices, and by the presence of fixed stations used as Roadside Units (RSUs), which provide connectivity to OBUs [25] (p. 225). At that stage of technology, the stable connections and mutual exchange of data between the network’s elements were not considered. Whereas VANETs are characterized by unstable, temporary networking (each node in VANETs is free to move independently and therefore changes to another node’s connection occur frequently [26]), the IoV consists of two interconnected ideas: the networking of vehicles and the development of smart vehicles. Consequently, the IoV aims to allow vehicles to communicate in real time with their human drivers’ devices, pedestrians’ devices, other vehicles, roadside infrastructure, and fleet management systems, which creates several types of network communication. The IoV, enabled by the IoT [27], allows vehicles to access a wide branch of data and information, e.g., the states of nearby vehicles, weather information, traffic status, etc. IoT technology allows the sharing of information collected via various smart devices and sensors allocated within and outside of the vehicles and consequently supports decision making processes for various stakeholders of traffic. By connecting vehicles to inter-vehicle networks, intra-vehicle networks, and the vehicular mobile internet, an IoT infrastructure application, referred to as the IoV [28], can be formed using traditional internet protocols and networks.

Because the IoV originates from VANETs, the “VANETs are classified into two categories: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications” [22], following [29]. It is now extended. When V2V is considered, it means that data and traffic-related information are exchanged between vehicles (communication between vehicles) [30]. Information and data related to the state of traffic can also be exchanged between vehicles and infrastructure—such a type of communication is abbreviated as V2I [30]. Historically, V2V and V2I first emerged from VANETs [22]; however, currently, the IoV supports five types of network communication: Intra-Vehicle (IV), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I); Vehicle-to-Cloud (V2C) and Vehicle-to-Pedestrian (V2P). General information regarding methods of communication for VANETs, V2Vs, V2Is, and V2Rs was developed in [31]. These five types of network communication are sometimes referred to as Vehicle to Everything (V2X) communication [32,33]. Such a term covers all possible current applications (see definitions in [34] given in Table 1). This is especially relevant for V2X communications that include location information and a set of certain data regarding other vehicles, RSUs, pedestrians, and cyclists [26]. The traffic management authority was added to the structure of V2X as a part of a secure data-sharing scheme for the IoV, which can significantly reduce the burdens on full-system resources ([35] after [36]). Therefore, the IoV term is heading towards V2X. The term Internet of Everything (IoX) is an extension of the IoT and is treated as a network of relations, data exchanges, and information flows between different machines through machine-to-machine (M2M) communication, other smart devices or equipment, people, and processes in real time [37]. The IoV is therefore one of the elements of the IoX set. M2M telematics was a significant step in the connected vehicles paradigm in 2005, leading to V2V becoming a reality [38] and the most extensive form of communication; i.e., V2X communication was presented in 2015 (the history of the IoV is well-developed in [38]).

Recently, Vehicle-to-Roadside units (V2R) have been mentioned in the literature as empowered by fog and edge computations [39,40] and thereby as taking the IoV to the next level. Fog computing provides a secure channel to allow the networks’ development into a fog system in terms of RSUs such as edge routers, intelligent traffic lights, and more [41]. Therefore, the V2R was incorporated into the list of broad IoV families. On the other hand, since the above-mentioned RSU devices are part of the infrastructure, it means that V2R is a part of V2I. Similarly, the terms Vehicle-to-Cellular Network communication (V2N) and Vehicle-to-Portable devices (V2P) have appeared [25] (p. 260). Nevertheless, the V2N may be treated as a part of the V2I set, along with V2R and V2P as Vehicle-to-Pedestrian (with the same above-mentioned abbreviation V2P).

More representatives are expected to appear in the V2X group soon. The next possibility is Vehicle-to-Grid (V2G), which serves as a connection between vehicles and the electricity grid and is relevant for electric vehicles (EVs). V2G is a communication interface for the bidirectional charging/discharging of EVs [25] (p. 292). However, according to [25] (p. 14), it is still in the design stage. The authors of [42] mentioned vehicle-to-home as another system that provides a managed, two-way current flow between the grid and vehicles.

To study definitions of the IoV, the following pseudo-code was applied in the Scopus database, directly as “definition” AND “internet of vehicles” AND (LIMIT-TO (EXACTKEYWORD, “Vehicle To Vehicle Communications”) OR LIMIT-TO (EXACTKEYWORD, “Vehicular Ad Hoc Networks”)) AND (LIMIT-TO (DOCTYPE, “re”)). Execution of the code resulted in 15 documents (it was decided that the review paper may become the most significant and complex when definitions are expected—this is the reason for document-type limitation in the above-mentioned pseudo-code). Before presenting the study on IoV definitions, it is worth mentioning what the main subjects of certain review papers were. The most common convergence point of the reviews focused on VANETs and were drawn from the following publications: [22,23,31,36]. The number of review papers on VANETs in comparison to the IoV may mean that any research on VANETs is treated as more serious, complex, and especially related to the historical values of the original term. The review paper [26] focused on autonomous vehicles, whereas the contributions [38,43] were directly concerned with IoVs in transportation and automation (it is worth underlining that in the case of [38] a timeline of IoV development was included). Meanwhile, in [44,45] the review process was mostly focused on V2V and V2I.

The definitions, given in Table 1, were divided into several cohorts. Firstly, it is worth mentioning definitions of the IoV given for specific purposes and drawn from specific assumptions, as in the case of [25,46]. The second cohort consists of definitions compiled through a conceptual transfer of various terms into the IoV, as with [47–49]. The next cohort consists of definitions given by applications [50]. The broad cohort reflects the cohort that defines the IoV through V2V or/and I2V [25] (p. 225), [44] (p. 17), [46] (p. 88), or in full-scale by V2X [25] (p. 259, 261). Finally, the cohort including direct IoV definitions consists of those given in [34,38].

**Table 1.** Definitions of IoV.

|  |  |  |
| --- | --- | --- |
| **Definition** | **Year of Publication** | **Reference** |
| “In the Internet of Vehicles, smart cars, equipped with both computational and communication resources, can provide intelligent vehicle control, traffic management and interactive applications.”  (the definition given by application) | 2022 | [50] |
| “In general, the vast revolution in the IoT (a system that enables objects such as sensors and actuators to communicate and talk with each other without human intervention to achieve a common goal) helped to reduce traffic accidents by embedding some IoT objects in vehicles; and this created the IoV concept [51].”  (the definition given through conceptual transfer of IoT) | 2020 | [48] |
| The IoV with big data technologies “creates new opportunities to diminish real-world problems such as traffic congestion, responsive and effective government processes for traffic monitoring, controlling, route management and urban planning etc.” | 2021 | [38] |
| “(…) an integration of three networks (…): an inter-vehicle network, an intra-vehicle network, and the vehicular mobile Internet.”  “(…) Internet of Vehicles plays a significant role in the safe delivery of goods as it enables realtime tracking of shipments, warehouse-capacity optimization, predictive asset maintenance, route optimization, and improved last-mile delivery”  (the definition given by application) | 2021 | Sukanya Mandal, IEEE member (India) quoted in [43] |
| “V2V communication enables vehicles to communicate directly with one another. This enables a vehicle to be alerted to the presence of other vehicles that are difficult for the vehicle to see”  (the definition given by V2V technology) | 2020 | [44] (p. 17) |
| “system for sharing vehicle-to-vehicle (V2V) information among vehicles to prompt appropriate driving control”  “infrastructure-to-vehicle (I2V) system is needed to communicate information among vehicles to prompt appropriate driving control”  (the definition given by V2V and I2V technologies) | 2020 | [45] (p. 88) |
| V2V: “OBUs communicate between themselves”  V2I: “OBUs communicate directly with RSUs”  (the definition given by V2V and I2V technologies) | 2020 | [25] (p. 225). |
| “Vehicle-to-Everything (V2X) technologies constitute the most critical and important components for communication infrastructure (between the consumer-vehicle-infrastructure-management center) to provide smarter, safer and faster travel in addition to the efficient use of the resources.”  (the definition given by V2X technology) | 2020 | [25] (p. 259) |
| “Vehicles exchange information with each other with the use of V2V communication and also access the network infrastructure through the Road Side Units (RSUs) or through the cellular network components e.g., eNodeBs (V2N communication).”  (the definition given by V2X technology) | 2020 | [25] (p. 261). |
| Vehicle connection with other infrastructures such as buildings, lights, stations, etc., is called Vehicle to Infrastructure (V2I) connection, while connecting vehicles with other vehicle systems are called V2V connection. The combination of both connection types V2I and V2V is known as Vehicle to Everything (V2X) connection. | 2018 | [52] |
| “The Internet of things (IoT) is a global network connecting smart objects and enabling them to communicate with each other. Whenever those smart objects being connected over Internet are e xclusively vehicles, then IoT becomes Internet of Vehicles (IoV).”  (the definition given through conceptual transfer of IoT) | 2018 | [47] |
| The definition given for specific purposes: “vehicles can broadcast information about their states to other vehicles (V2V), including speed, heading, and location, as well as the information related to the environment while adverse weather conditions or obstacles can be acquired from infrastructure (V2I).”  “In vehicle-to-infrastructure (V2I) systems, the vehicles communicate with RSUs or cellular base stations at fixed positions. This allows the RSUs to communicate their location, weather conditions, traffic flow, etc. with vehicles to estimate their own position more accurately.” | 2018 | [26] |
| “The Social Internet of Vehicles (SIoV) is an example of a SIoT [SIoT stand for Social Internet of Things—added by this papers authors] where the objects are smart vehicles (mostly cars). The social connections can be made between vehicles, drivers and other users and between these two groups.”  (the definition given through conceptual transfer of IoT) | 2015 | [49] |
| “Providing wireless connectivity to vehicles enables communication with internal and external environments, supporting vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-sensor, and vehicle-to-Internet communications”  (the definition given for specific purposes) | 2014 | [26,46] |
| “The Internet of Vehicles (IoV) is an integration of three networks: an inter-vehicle network, an intra-vehicle network, and vehicular mobile Internet. Based on this concept of three networks integrated into one, we define an Internet of Vehicles as a large-scale distributed system for wireless communication and information exchange between vehicle2X (X: vehicle, road, human and internet) according to agreed communication protocols and data interaction standards (examples include the IEEE 802.11p WAVE standard, and potentially cellular technologies). It is an integrated network for supporting intelligent traffic management, intelligent dynamic information service, and intelligent vehicle control, representing a typical application of Internet of Things (IoT) technology in intelligent transportation system (ITS).” | 2014 | [34] |

The design of the IoV must be sustainable. The three pillars of ESG are essential for a sustainable IoV and should be supported. Sustainability is impossible if one of the components of sustainable development is not supported. These three components are informally referred to as planet, people, and profits. Although the three should be equally supported, environmental (planet) and economic (profits) tend to be more dominant than the social component (people). This is wrong because the social component affects the quality of life and well-being of individuals more than environmental issues. Furthermore, sustainability requires a balance between all the pillars. Sustainable IoV design needs social sustainability as much as the rest of the ESG pillars.

3. ESG in IoV Design and Application

3.1. IoV: An Environmental Perspective

The environmental perspective in the context of the IoV is an extremely broad topic. A search of relevant scientific databases revealed 521 publications indexed on the Web of Science (the pseudocode: *(ALL = (“internet of vehicles”)) AND ALL = (environment)*) in recent years, i.e., 2010–2022 (date of data collection: 10 May 2022). A much more sizable sample was registered in the Scopus database, i.e., 8358 publications (*ALL(“internet of vehicles”) AND ALL (environment)*), in recent years, i.e., 2014–2022 (date of data collection: 27 October 2022). Based on results obtained using both databases, a method known as a scoping review was applied to determine the types of environments considered in each publication.

Firstly, the list of publications related to different semantic types of environmental terms is presented in this section. Secondly, below the list, the most interesting publications related to the environment, as a part of the ESG concept, are mentioned in more detail.

The authors of publications broadly discuss “environment” as follows:

* Devices and software environments (including IoV network environments, V2X environments, etc.), namely systems involving IoV technology. In general, that type of “environment” can be summed up as a software and/or hardware environment [53–72] (in [66], a network environment is understood by its parameters as a quantity of vehicles, load, speed, etc.). An interesting application of IoV control methods in the context of device and software environments is given in [73], where the authors developed a smart terminal-box for unmanned earthwork machinery (including bulldozers, graders, and rollers) which works in the tough environments of varied weather. Additionally, it may be underlined here that the authors of [74] mentioned blockchain to be envisioned as a type of enforcement applied to ensure trustworthiness in diverse IoT environments (and consequently in IoV environments, which is a subject matter of [75]).
* Internal and external environments of an organization, e.g., the manufacturing environment, the supplier’s competitive environment, the sales competition environment, and the customer usage environment as mentioned in [76].
* An environment as acreage was given in [77].
* Some other publications treat the environment as an infrastructural network [78–80], as a surrounding [81–86], and as an (urban) traffic environment [70,87–91].
* A small environment, as in the concept in biology, was applied to the IoV by [92].
* An environment consisting of vehicles, tasks, wireless channels, and mobile edge computing servers was mentioned in [93].
* Various types of environments were mentioned in [94], without any unification.

It is worth mentioning that, in numerous papers among the analyzed sample, IoV and environment terms appeared sporadically in the body of the publication or in the listed references—such publications have been omitted and not included in the above-mentioned list.

As can be observed from the above-presented list, most of the publications related to the IoV and the environment regard the environment differently. It can be treated as a space, network, system, and as its components’ function (road system environment, vehicle system environment, vehicular environment). Hence, the number of publications with the keyword “environment” is huge. Consideration of the IoV from the point of view of environmental protection and the ecology-related environment happens far less frequently.

Pro-environmental perspectives on IoV technologies are certainly related to the elimination of energy and signal loss during routing data between devices and the reduction of power consumption across the IoT network. The authors of [95] developed a method to eliminate energy loss in IoT technology thanks to the optimal path of signal flow, which certainly can also be applied to the IoV. This can benefit environmental aspects in two ways. On the one hand, the issue is related to the elimination of energy losses; on the other hand, the sensors in the proposed method, based on Fuzzy Logic coupled with the Grasshopper Optimization Algorithm, provide numerical data which can be used for environment monitoring (weather, health, security, etc.) [95]. Furthermore, [96,97] proposed routing protocols to maintain efficient energy consumption in the described technology and in relation to the issues mentioned above. The problem of signal and data flow delays was considered in [98] as well. The authors proposed mixed-integer linear programming to minimize cloud delay between hosts, treating it as a joint optimization algorithm (in contrast to single algorithms as the delay optimization algorithm and host optimization algorithm, respectively). Additionally, in [99] the authors worked on increasing reliability and decreasing delays in V2V and V2I connections within the dynamic changing environment, and they developed an algorithm with a certain success rate. Cloud networks without consideration of delays were developed in [100].

The environmental aspects of the IoV were indirectly mentioned in [101]. The authors, considering V2G, mentioned the environmental impact of V2G design objectives and closed their paper with this statement: “in this age of environmental degradation, we need a reasonable amount of renewable energy.” This has been an important topic among IoV applications in V2H and V2G since V2H uses the energy stored in electric vehicles to power household appliances, while V2G allows the energy stored in these vehicles to be released to the grid [42]. The IoV, along with hybrid electric vehicles, is also treated as an input to energy problems in [102].

A final thought related to the environmental perspective considers ESG itself. According to [103], vehicles, thanks to IoV technology, can act as sensing points whose measurement results ensure more services, safety, and efficiency for transportation systems [104]. Yet, importantly, from the viewpoint of ESG the IoV provides sensors for environmental conditions which can meet the needs of smart cities.

In [105], it was mentioned that the IoT has been outlined as comprising “[t]hings that have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within the social, environmental, and user contexts” [106]. Apparently, the environmental aspect of the IoT was noted years ago (2010); nevertheless, it has not yet been researched enough. The shaping of such an approach can be expected to increase in the near future. In particular, the authors of [107] recently discussed how the cloud-based Connected Autonomous Vehicles Ecosystem can support superior traffic management and reduce CO2 emissions. This result was found in a review paper related to IoT technology for the Connected Autonomous Vehicles Ecosystem by [108].

To sum up the section, it should be underlined that far too little attention is paid to the environmental aspects of the IoV, not enough attention is paid to signal loss, and there is practically no research on the actual costs of the Internet, which, like the external costs of transportation, are very difficult to estimate.

3.2. IoV: A Social Perspective

The social perspective in the context of the IoV is almost as broad a topic as the environmental perspective. As in the previous section, the relevant scientific databases were taken into consideration and the quantitative results were as follows. The pseudocode *(ALL = (“internet of vehicles”) AND ALL = (social))* applied in recent years, i.e., 2010–2022 (date of data collection: October 27th, 2022), revealed 29 publications solely for the Web of Science database. Therefore, based on the preliminary investigation, the search was modified to “*social internet of vehicles*”, which was applied to all fields of the database records, revealing 62 publications. The Scopus database was investigated similarly. Consequently, when the first given pseudocode was checked in Scopus, it resulted in 5837 publications of different natures. In contrast, the search with the phrase “*social internet of vehicles*” applied to all fields of the database records resulted in 1200 publications. These publications constituted a database that was first used for a scoping review; secondly, the most significant publications presenting the social perspective of the IoV were investigated to a greater extent.

The research group [109] presented different options for socializing vehicles and other entities (including passenger socializing, e.g., in public communication) connected to the VANET, namely via the internet, Dedicated Short-Range Communication (DSRC), or other communication technologies. Such socialization is understood as sharing cohorts of data grouped by traffic information/traffic efficiency, weather conditions, road situations/road experience, toll gates, vacant car parking slots, road safety, travel comfort, entertainment along the roads, and media sharing [109–111]. Some authors relied on the social internet of vehicles (SIoV) as a composition of social networks and the IoV [112]. An interesting observation was given in [113]—the SIoV was compared to human semi-social behavior, was not completely trusted, and was seen to be potentially filled with adverse, malicious information. This leads to interesting ethical dilemmas, as mentioned in [111], which are indirectly related to the SIoV yet directly related to autonomous vehicles. Namely, “1) If driverless cars are not safer than human drivers it will be unethical to sell them. 2) Once driverless cars are safer than human drivers (reduce the risks to third parties), driving will be unethical” [111,114]. Socialization of the IoV can be treated as building a network of various devices which care about the protection of privacy and security in the SIoV, as mentioned in [109,115–117].

The key exchange protocol was mentioned in [118] as the most common protocol among security solutions. The authors’ continuous challenge was focused on desired performance and security properties which were unsatisfactory, whereas the key exchange protocol developed in [118] had an 84% improvement in execution time and a 54% improvement in communication overhead. The authors of [119] noted that the mentioned security problem for the SIoV is still unsolved; however, they commented as well that standardization organizations agreed to apply Vehicular Public-key Infrastructure (V-PKI) to SIoV security. According to [120], the technology related to Artificial Intelligence (AI) was the technology that led the IoV to the next phase of intelligence, namely the SIoV, which makes the issue of privacy and security of exchanged data even more serious. SIoV security contributed to a decrease in vehicle crashes by 80% [109,119,121,122]. Some algorithms related to SIoV security were given in [119]. These were, for example, developed using Unmanned Aerial Vehicles (UAV) to secure the SIoV, as presented in [123] (UAVs were also investigated in [110] to assist the mobile edge computing environment compared to the SIoV). The same authors mentioned that the goal of the SIoV, also known as a vehicular social network (VSN), is to “make vehicles capable of social communication and low-cost infotainment service provisioning, by integrating social networking-related concepts into IoV” [124]. Relations between vehicles and aspects of road infrastructure, including effective, low-cost, and flexible solutions, were also given in [20]. Movable entities were also treated as event witnesses—the authors of [125] developed incentive-based vehicle witnesses as services that treat vehicles moving in an ad hoc network as witnesses to designated events.

The authors of [126] considered the SIoV in the context of its application of controlling traffic congestion and road safety, and they have developed an algorithm supporting that concept. The authors of [127] improved traffic efficiency by timely delivery of data/information in the SIoV environment with ultra-high-speed integrated cellular 5G technologies (or any other traditional communication technologies such as Wi-Fi, cellular networks, or through dedicated short-range communication [111]). Instead of 5G technologies, the authors of [128] proposed a DigiMesh radio module for an ad hoc wireless network in the SIoV to transmit and receive alerts on the driving behaviors of nearby vehicles. The improved performance of a collaborative edge computing-based traffic management system was the goal in [129], aiming specifically to reduce the average waiting time of vehicles in a network, especially in intersections. For this purpose, multi-agent-based deep reinforcement learning was applied to the interaction of servers with IoV and traffic lights to prompt dynamic green waves. Furthermore, in [130], the traffic congestion (gaining the maximum throughput) was supported by application of the dynamic traffic congestion management algorithm within the SIoV, although it was developed especially for intersections.

The continued connection (even temporarily established) between interconnected entities relies on trustworthiness, which is one of the urgent issues that must be addressed for wireless connections [131]. This is the case especially since connections in the SIoV are characterized by the ad hoc nature of the environment [132] (the authors focused on the trustworthiness algorithm in the SIoV). Other authors also added scalability and navigability to trustworthiness as key challenges of the SIoV, mentioning that it is still at an early stage of development [133]. Moreover, standardization, adaptability, infrastructure, and lack of applications were given as topics worth analyzing in addition to the above-mentioned issues [134]. In relation to trust and security in the SIoV network, the authors of [135] investigated a trust-aware, social in-vehicle and inter-vehicle communications architecture which showed promise during simulation experiments. The end-fog-cloud system architecture was applied in the mentioned publication. Fog computing-based systems continually raise interest in the SIoV area. The authors of [136,137] investigated a dual-mode data forwarding SIoV scheme based on interest tags for a fog computing-based SIoV. Experimental results validated the efficiency and stability of forwarded data and information. The first ideas regarding algorithms and models for dynamic audits of the correctness of shared data in extremely fast changes of entities in SIoV systems were developed in [138]. This was the research that envisioned the transformation of the IoV into the SIoV, according to the authors.

Another aspect of the SIoV is the building of its model. The model and SIoV scenarios were identified in [139] (the authors mentioned that they extended the concept of SIoT to the IoV, proposing SIoV). The detailed architecture of the SIoV was presented in [49] together with an interesting vision that the SIoV will be applied to smart cities. The authors of [140] proposed a device-to-device enabled SIoV model consisting of vehicles, RSUs, base stations, traffic management servers, and trust authority (a taxi trajectory simulation-based analysis was included in the research). A similar model was given in [127]. Data privacy and data protection were also of interest in [141]—the authors focused their research on the Conditional Choice Probability-Federated Deep Learning algorithm to increase trust in a chain of involved entities. Meanwhile, the authors of [142] presented a decentralized scheme for solving the peer disclosure issues in the SIoV. They applied a directed, acyclic, graph-based mutual supervision algorithm assuring 72% multi-dimensional privacy against leakage of transmitted images in comparison to non-peer disclosure prevention. Prevention of data leakage was also of interest in [143], in which authors proposed a federated learning collaborative authentication protocol for shared data which had the lowest authentication delay in comparison to other protocols and in which the data packet loss rate was reduced to 4.68%. The potential of federated learning was first observed in [144], where addressing data privacy and data trajectory in SIoV networks was taken into consideration under simulation methods.

In the survey [145], a comparative analysis of models related to location privacy protection was developed. These models were based on user attribute information, user behavior information, and user relationship networks. Location privacy protection of SIoV users can also be ensured with a method based on double k-anonymity, the goal of which is to hide users’ locations and requested information—such a concept was given under simulation by the same group of authors in [146]. Continuous work on SIoV safety led the authors of [147] to a statement that their authentication protocols can be of higher resistance in comparison to authentication protocols given in [148], which are treated as more vulnerable to internal attacks and smart card theft attacks and which lack perfect forward security.

Data transmission, data delivery, and minimization of buffer occupancy were developed with up-to-date algorithms (e.g., the susceptible-infected-recovered model) in [149]. Such challenges, mentioned as well in the above-quoted research, led to green computing in the SIoV (i.e., networks virtualization, use of the cloud, energy saving), as it was called in [150]. To increase such green traffic data dissemination in the SIoV, the authors of [151] adopted a meta-heuristic solution which consists of two-way particle swarm optimization.

Congestion challenge is not solely related to traffic in the case of SIoV application. The authors of [152] noted that Transmission Control Protocol/Internet Protocol (TCP/IP)-based congestion control mechanisms cannot be directly applied in the IoV environment. The reason is the need for high throughput and low delays in signal transition, which are hardly obtained for content-sharing in some cases. The authors developed the sharing system in the SIoT network without vehicle IP assignment. The security of communication in the SIoV environment is ensured by blockchain. Blockchain technology was also applied to ensure not only security but also privacy in research developed by the authors of [153].

There is no one focus point in the SIoV. Trustworthiness [131,132,135], security [118, [119,120,123,135,153], safety [126,128], privacy [142–144,146,153], scalability [133], and computing capacity [127,136–138,149,152] are among the most common and continuous challenges related to the SIoV. These issues are compounded by the low communication efficiency and high computational cost of the SIoV. Fog computing [136,137,150] (together with or in contrast to edge computing [110,129,144]) is therefore foreordained to improve performance and reduce the amount of data sent to the cloud for processing, analysis, and storage. It can also be used for security reasons and to address the need to comply with applicable data processing regulations.

3.3. IoV: A Governance Perspective

One of the underpinning purposes of the IoV, based on the assumption that vehicles are always, or almost always, connected to the Internet, is to expand the services and information flow that users may use and benefit from while traveling in their vehicles. These services include a variety of roles that intelligent vehicles will be engaged in, such as customer roles and database roles, as well as the collecting and distributing of big data resources [4]. This purpose led to the paradigm of the social network of vehicles (i.e., SIoV), in which anonymous relations are established between vehicles and road infrastructure equipment [20]. This in turn created the potential for social innovations for sustainable transport and infrastructure [3]. Moreover, the data gathered from the surrounding world, other vehicles, and drivers has facilitated the smooth operation of Autonomous Vehicle Systems, environmental protection, and road traffic [4].

However, such an approach carries governance risks which need to be addressed and managed well for IoV solutions to succeed. These are, among others:

* Data security and information privacy;
* Lof personal data and personal privacy;
* Compliance with the GDPR;
* Serious security breaches related to the broadcasting of false alarms;
* Limited effectiveness of IoV systems related to poorly managed private data sharing in the cloud [154–159].

Many potential solutions can help to solve the above-described governance and security challenges. For example:

* Blockchain-based IoV network architecture aims to protect connected vehicles from attacks and is based on a sophisticated secure IoT network [160].
* Policy hidden attribute-based encryption with dynamic service (PH-ABE-DS) and edge-assisted policy hidden attribute-based encryption with dynamic service (EA-PH-ABE-DS) are two solutions dealing with internal and external security issues that simultaneously offer an appropriate level of usability and enable full policy hiding [154].
* Blockchain solutions can support high privacy levels, preserve full data disclosure, and facilitate lower costs for owned redundant storage and related procedures [158].
* False alarm detection methods, e.g., outlier detection, intrusion detection, the detection of security attacks, inconsistency detection applied to communicating, and messages misbehavior detection are relevant [29,155] (these methods were developed through the application of a hidden Markov model-based prediction framework based on a probabilistic model).
* PPIoV (i.e., Privacy Preserving-based framework for IoV-fog environment) is a federated learning and blockchain-based method aimed at ensuring the short information processing times which are necessary for the IoV environment, as well as ensuring trust [157].

Another serious governance-related challenge consists of a variety of potential attacks that can affect IoV networks and infrastructure and target availability, authentication, data integrity, confidentiality, and routing. These include, among others, channel interference attacks, Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, message tampering attacks, eavesdropping attacks, malware attacks, message holding attacks, sybil attacks, masquerading/impersonation attacks, wormhole/tunneling attacks, GPS spoofing attacks, replay attacks, message manipulation attacks, and route modification attacks [161]. These attacks can be managed thanks to many different solutions acting as remedies. These are, for example, group signatures, event-based reputation systems, session key certificates, footprints, identity-based cryptography, digital certificates, timestamps, and geographical leashes [161–164]. However, due to a wide variety of potential threats and solutions, this task is not easy. In order for the task to be successful, the potential threats and solutions must be well-selected, deeply understood, and properly implemented in line with their primary aim. Another option to deal with attacks is to predict and prevent them. An example of such a solution is a real time learning model for early prediction of phishing attacks in the IoV [165].

Last, but not least, it is also worth noting that this scoping review proves that blockchain seems to be a promising technology that may solve or help mitigate governance problems related to the IoV, e.g., [166–171]. It is also currently the most popular among researchers, e.g., [172–175].

The governance issues listed above are the most important and the most common in the literature. Due to the significantly growing interest of scholars and practitioners in the IoV, the number of IoV-related publications is growing significantly and quickly. Nonetheless, most of the papers are technical and describe technologies supporting the IoV and thus are not relevant to this part of the study. The governance perspective of the IoV presented in this section is based on the results of a scoping review performed on the Scopus database search (date of data collection: 27 October 2022). The following keywords were shuffled in multiple searches: IoV, governance, privacy, data, and risk:

* *(TITLE-ABS-KEY ( iov ) AND TITLE-ABS-KEY ( governance ) )*; four documents; 2019–2022;
* *(TITLE-ABS-KEY ( iov ) AND TITLE-ABS-KEY ( data ) AND TITLE-ABS-KEY ( privacy ) )*; 230 documents; 2013–2023, where 91% of publications is dated from 2019 to 2023;
* *(TITLE-ABS-KEY ( iov ) AND TITLE-ABS-KEY ( data ) AND TITLE-ABS-KEY ( risk ) )*; 83 documents (2007–2022), where 78% of publications was dated from 2019 to 2022.

The publications included in the scoping review were dated from 2019 to 2023, and published in English as articles, conference papers, reviews, or conference reviews. The final sample was composed of 266 publications and all of those constitute the background of this analysis. After the initial screening of titles, abstracts, and keywords, 32 articles were selected as matching the goals of this section and were deeply analyzed, as presented above.

4. Discussion

The analysis conducted in this paper shows that the knowledge base about the IoV and related concepts is considerably broad and interdisciplinary. Thus, it needs a synthesis. The growing importance of maintaining the sustainability of transportation led to the analysis and further explanation of the IoV concept based on three different dimensions related to sustainability—the environmental, social, and governance perspectives (ESG).

The above-mentioned perspectives present a holistic picture of IoV dimensions. It shows that the three ESG perspectives not only constitute individual pillars of the IoV, but also overlap in various ways and therefore should be addressed together to support the complex IoV transformation toward sustainability. The interconnections between these three perspectives appear to be strong, and it is useful to address them simultaneously.

The environmental dimension covers issues related to, among others:

* The elimination of energy losses;
* Data which can be used for environmental monitoring (weather, health, security, etc.);
* Routing protocols to maintain efficient energy consumption;
* A reasonable amount of renewable energy for IoV issues;
* The IoV next to hybrid electric vehicles as an input to energy problems;
* Vehicles, thanks to IoV technology, acting as sensing points whose measurement results ensure more services, safety, and efficiency for transportation systems;
* IoV sensors for environmental conditions, which can meet the needs of smart cities;
* Systems supporting superior traffic management and CO2 emissions reduction.

The social dimension is grounded in interactions at various levels and can be seen as a composition of social networks and the IoV. It poses challenges related to SIoV trustworthiness, security, safety, privacy, scalability, and computing capacity. Socialization of the IoV means sharing cohorts of data grouped in traffic information/traffic efficiency, weather conditions, road situations/road experience, toll gates, vacant car parking slots, road safety, travel comfort, entertainment along roads, and media sharing. It can be compared to human semi-social behavior created by a network of various devices attuned to the protection of privacy and security. This security aspect seems to be important, especially since these connections rely on social communication for vehicles with a need for scalability and navigability to transmit and receive alerts on driving behaviors and green traffic data dissemination. This dimension of the IoV seems to be crucial in supporting social innovations for sustainable transport and infrastructure.

The environmental and social dimensions are bounded by governance-related issues addressing mainly:

* Data security and information privacy;
* Data leakage;
* Personal privacy and compliance with the GDPR;
* Serious security breaches related to the broadcasting of false alarms;
* Limited effectiveness of IoV systems related to poorly managed private data sharing in the cloud;
* A variety of potential attacks that can affect IoV networks and infrastructure and target availability, authentication, data integrity, confidentiality, and routing.

All of these interconnections, if managed wisely, can surely support a more holistic and complex perspective on IoV systems, including their better design and more thought-through implementation.

5. Conclusions and Future Research Directions

The ESG perspective is interlocked. Each perspective is represented as a puzzle piece in the graphic representing the results of the presented considerations (Figure 1). At the same time, the individual ESG perspectives are represented as cells in a honeycomb—they interconnect, intermingle, and at the same time allow for the inclusion of future, yet-to-be-defined concepts, and extend beyond the IoV. In addition, Figure 1 includes a layer-based architecture of the IoV system based on [176].



**Figure 1.** Allocation of ESG perspectives and related issues within the conceptual model of IoV systems. Source: the layer-based architecture of the IoV system based on [176].

The overlapping puzzle pieces indicate that within each layer in the IoV system design process, all perspectives should be considered together. However, based on the conducted analyses, it appears that IoV issues are either not sufficiently discussed in the context of each perspective or are omitted in the discourse (it is also worth noting here once again how heterogenous a perspective can be considered, including, for example, the diverse understanding of the term “environment” given in Section 3.1). For example, the issue of communication overhead has so far been considered in the context of environmental and corporate governance perspectives to the exclusion of social ones. To ensure the sustainability of IoV systems, each perspective should be considered. Moreover, this work has to be conducted by various stakeholders whose actions can positively impact the sustainability of the IoV at various levels. For example, by developing and promoting more sustainable solutions, industry players can affect their application rate. Regulators supporting such adoption with relevant laws and procedures can facilitate their wider diffusion, whereas governments, thanks to targeted policy measures, may incentivize this process. Certainly, the development of the IoV raises various ethical concerns related to privacy, security, and social justice. These should be treated seriously and considered at all levels of IoV solutions development, implementation, and usage. However, thanks to novel IT systems and good data management and storage, such a problem can be minimalized and hopefully, in time, even definitely resolved. All the perspectives should be included within the design of networks intended to cooperate as IoV systems. An approach of this type, albeit just in its infancy, can be seen within the cohort of publications analyzed. This approach applies to the issues concerning each of the perspectives, and these are:

* Environmental factors monitoring;
* Supporting traffic management;
* Reducing CO2 emissions;
* Sharing cohorts of data.

The remaining identified issues are either related to only one perspective (e.g., the issue of energy loss) or at most two perspectives at the same time (e.g., the communication overhead). Therefore, it is worth stating that future research agendas should move toward specific perspectives, as described below.

For future research agendas, it would be desirable to steer the following issues toward a corporate governance perspective (in the case of these issues, the other two perspectives have already been considered):

* Signal and data flow delays and execution time;
* Energy loss.

On the other hand, the following issues should be directed toward the social perspective (again, the other perspectives have already been considered for these issues):

* Communication efficiency, computational cost, and expenditures;
* Data security and information privacy;
* Communication overhead;
* Security and data processing regulations;
* Energy loss.

Certainly, at the same time, it is recommended that existing research directions be sustained.

**Author Contributions:** M.K. and L.U. proposed the idea; M.K. edited the manuscript; M.K. and M.M. conducted the literature review and arrived at the results; introduction, M.M.; literature review, M.K. (67%) and M.M. (33%); materials and methods, M.K. and M.M.; data curation M.K.; graphics M.K.; results, M.K. and M.M.; conclusion, M.K.; writing—original draft, M.K. and M.M.; visualization, M.M.; final revision, M.K., M.M., and L.U. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Not applicable.

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

References

1. Balasubramaniam, A.; Paul, A.; Hong, W.-H.; Seo, H.; Kim, J.H. Comparative Analysis of Intelligent Transportation Systems for Sustainable Environment in Smart Cities. *Sustainability* **2017**, *9*, 1120. https://doi.org/10.3390/su9071120
2. Balasubramaniam, A.; Paul, A. Comparative study of sustainable transportation systems: A futuristic approach. ICSNS 2018 - Proceedings of IEEE International Conference on Soft-Computing and Network Security 2018; Coimbatore, India, 14 – 16 February 2018*;* Curran Associates: Ney York, NY, USA.https://doi.org/10.1109/ICSNS.2018.8573649
3. Aamir, M.; Masroor, S.; Ali, Z.A.; Ting, B.T. Sustainable Framework for Smart Transportation System: A Case Study of Karachi. *Wireless Personal Communication* **2019**, *106*, 27–40. http://doi.org/10.1007/s11277-019-06259-4
4. Hussain, H.I.; Kamarudin, F.; Mohd-Sanusi, Z.; Shuhidan, S. M.; Saad Al-Dhubaibi, A. A.; Ahmad Razimi, M.S. Governance in the internet of vehicles (IoV) context: Examination of information privacy, transport anxiety, intention, and usage. *Journal of Advanced Transportation* **2021**, 5563260. http://doi.org/10.1155/2021/5563260
5. Zhao, L.; Jia, Y. Intelligent transportation system for sustainable environment in smart cities. *International Journal of Electrical Engineering & Education* **2021a**, 1–19. https://doi.org/10.1177/0020720920983503
6. Eccles, N.; Viviers, S. The Origins and Meanings of Names Describing Investment Practices that Integrate a Consideration of ESG Issues in the Academic Literature. *Journal of Business Ethics* **2011**, *104*(3), 389–402. http://dx.doi.org/10.1007/s10551-011-0917-7
7. Nirino, N.; Santoro, G.; Miglietta, N.; Quaglia, R. Corporate controversies and company’s financial performance: Exploring the moderating role of ESG practices. *Technological Forecasting and Social Change* **2021**, *162*, 120341. https://doi.org/10.1016/j.techfore.2020.120341
8. Capelle-Blancard, G.; Petit, A. Every Little Helps? ESG News and Stock Market Reaction. *Journal of Business Ethics* **2019**, *157*(2), 543–565. http://dx.doi.org/10.1007/s10551-017-3667-3
9. Daugaard, D. Emerging new themes in environmental, social and governance investing: a systematic literature review. *Accounting & Finance* **2020**, *60*(2), 1501–1530. http://dx.doi.org/10.1111/acfi.12479
10. Friede, G. Why don’t we see more action? A metasynthesis of the investor impediments to integrate environmental, social, and governance factors. *Business Strategy and the Environment* **2019**, *28*(6), 1260–1282. http://dx.doi.org/10.1002/bse.2346
11. Cordeiro, J.J.; Profumo, G.; Tutore, I. Family ownership and stockholder reactions to environmental performance disclosure: A test of secondary agency relationships. *Business Strategy and the Environment* **2021**, *30*(4), 2091–2107. http://dx.doi.org/10.1002/bse.2734
12. Mukandwal, P.S.; Cantor, D.E.; Grimm, C.M.; Elking, I.; Hofer, C. Do Firms Spend More on Suppliers That Have Environmental Expertise? An Empirical Study of U.S. Manufacturers’ Procurement Spend. *Journal of Business Logistics* **2020**, *41*(2), 129–148. http://dx.doi.org/10.1111/jbl.12248
13. Fritz, M.M.C.; Ruel, S.; Kallmuenzer, A.; Harms, R. Sustainability management in supply chains: the role of familiness. *Technological Forecasting and Social Change* **2021**, *173*, 121078. http://dx.doi.org/10.1016/j.techfore.2021.121078
14. Brooks, C.; Oikonomou, I. The effects of environmental, social and governance disclosures and performance on firm value: A review of the literature in accounting and finance. *British Accounting Review* **2018**, *50*(1), 1–15. http://dx.doi.org/10.1016/j.bar.2017.11.005
15. Grant, M. J.; Booth, A. A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies. *Health Information & Libraries Journal* **2009**, *26*(2), 91–108. http://dx.doi.org/10.1111/j.1471-1842.2009.00848.x
16. Daudt, H. M.; van Mossel, C.; Scott, S.J., Enhancing the Scoping Study Methodology: A Large, Inter-Professional Team’s Experience with Arksey and O’Malley’s Framework. *BMC Medical Research Methodology* **2013**, *13*(1). http://dx.doi.org/10.1186/1471–2288–13–48
17. Colquhoun, H.L.; Levac, D.; O’Brien, K.K.; Straus, S.; Tricco, A.C.; Perrier, L.; Kastner, M.; Moher D. Scoping Reviews: Time for Clarity in Definition Methods, and Reporting. *Journal of Clinical Epidemiology* **2014**, *67*(12), 1291–1294. http://dx.doi.org/10.1016/j.jclinepi.2014.03.013
18. Zia, K.; Muhammad, A.; Khalid, A.; Din, A.; Ferscha, A. Towards Exploration of Social in Social Internet of Vehicles Using an Agent-Based Simulation. *Complexity* **2019**, 8201396. https://doi.org/10.1155/2019/8201396
19. Talib, M.A.; Abbas, S.; Nasir, Q.; Mowakeh, M.F. Systematic literature review on Internet-of-Vehicles communication security. *International Journal of Distributed Sensor Networks* **2018**, *14*(*12*). https://doi.org/10.1177/1550147718815054
20. Atzori, L.; Floris, A.; Girau, R.; Nitti, M.; Pau, G. Towards the implementation of the Social Internet of Vehicles. *Computer Networks* **2018**, *147*, 132–145. https://doi.org/10.1016/j.comnet.2018.10.001.
21. Yang, F.; Wang, S.; Li, J. Liu, Z.; Sun, Q. An overview of Internet of Vehicles. *China Communications* **2014**, *11*(*10*), 1–15. https://doi.org/10.1109/CC.2014.6969789.
22. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). Sensors **2019**, 19, 3589. https://doi.org/10.3390/s19163589.
23. Xu, X.; Wang, Y.; Wang. P. Review Article Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks. *Journal of Advanced Transportation* **2022**, 4725805. https://doi.org/10.1155/2022/4725805
24. Mejri, N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications* **2014**, *1*(*2*), 53–66.
25. Mouftah, H.T., Erol-Kantarci, M., & Sorour, S. (Eds.). Connected and Autonomous Vehicles in Smart Cities, 1st ed. CRC Press: Boca Raton, FL, USA 2020. https://doi.org/10.1201/9780429329401
26. Kuutti, S.; Fallah, S.; Katsaros, K.; Dianati, M.; Mccullough, F.; Mouzakitis, A. A Survey of the State-of-the-Art Localization Techniques and Their Potentials for Autonomous Vehicle Applications. *I*EEE Internet of Things Journal **2018**, *5* (*2*), 829–846. https://doi.org/10.1109/JIOT.2018.2812300.
27. Minerva, R.; Biru, A.; Rotondi, D. Towards a Definition of the Internet of Things (IoT). *IEEE Internet Initiative* **2015**, *1*, 1–86.
28. Fangchun, Y.; Shangguang, W.; Jinglin, L.; Zhihan, L.; Qibo, S. An overview of Internet of Vehicles. *China Commun.* **2014**, *11* (*10*), 1–15. https://doi.org/10.1109/CC.2014.6969789
29. Dua, A.; Kumar, N.; Bawa, S. A systematic review on routing protocols for Vehicular Ad Hoc Networks. *Veh. Commun.* **2014**, *1*, 33–52. https://doi.org/10.1016/j.vehcom.2014.01.001
30. Liu, K.; Ng, J.K.Y.; Lee, V.C.S.; Son, S.H.; Stojmenovic, I. Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network. IEEE/ACM Transactions on Networking **2016**, *24*(*3*), 1759–1773. https://doi.org/10.1109/TNET.2015.2432804.
31. Chahal, M.; Harit, S.; Mishra, K.K.; Sangaiah, A.K.; Zheng, Z. A Survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. *Sustainable Cities and Society* **2017**, *35*, 830–840. https://doi.org/10.1016/j.scs.2017.07.007.
32. Wang, J.; Shao, Y.; Ge, Y.; Yu, R. A Survey of Vehicle to Everything (V2X) Testing. *Sensors* **2019**, *19*, 334. https://doi.org/10.3390/s19020334
33. 5G Americas. March 2018. Cellular V2X Communications Towards 5G. Available online: http://www.5gamericas.org/en/resources/white-papers/(accessed on 12 June 2022).
34. White Paper of Internet of Vehicles (IoV). Available online: http://mddb.apec.org/Documents/2014/TEL/TEL50-PLEN/14\_tel50\_plen\_020.pdf (accessed on 4 June 2022).
35. Kong, Q.; Lu, R.; Ma, M.; Bao, H. A privacy-preserving sensory data sharing scheme in Internet of Vehicles. *Future Gener. Comput. Syst*. **2019**, *92*, 644–655. https://doi.org/10.1016/j.future.2017.12.003
36. Sun, X.; Yu, F.R.; Zhang, P.; Xie, W.; Peng, X. A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks. Sensors **2020**, 20, 4253. https://doi.org/10.3390/s20154253
37. Langley, D.J.; van Doorn, J.; Ng, I. C.L.; Stieglitz, S.; Lazovik, A.; Boonstra, A. The Internet of Everything: Smart things and their impact on business models. *Journal of Business Research* **2021**, *122*, 853–863. https://doi.org/10.1016/j.jbusres.2019.12.035.
38. Arooj, A.; Farooq, M.S.; Akram, A.; Iqbal, R.; Sharma, A.; ·Dhiman, G. Big Data Processing and Analysis in Internet of Vehicles: Architecture, Taxonomy, and Open Research Challenges. *Archives of Computational Methods in Engineering* **2022**, *29*, 793–829. https://doi.org/10.1007/s11831-021-09590-x
39. Lyamin, N.; Kleyko, D.; Delooz, Q.; Vinel, A. AI-Based Malicious Network Traffic Detection in VANETs. *IEEE Netw*. **2018**, *32*, 15–21. https://doi.org/10.1109/MNET.2018.1800074.
40. Keshari, N.; Singh, D.; Maurya, A.K. A survey on Vehicular Fog Computing: Current state-of-the-art and future directions. *Vehicular Communications* **2022**, *38*, 100512. https://doi.org/10.1016/j.vehcom.2022.100512.
41. Zhang, L. Key Management Scheme for Secure Channel Establishment in Fog Computing. *IEEE Trans. Cloud Comput*. **2021**, *9*(*3*), 1117–1128. https://doi.org/10.1109/TCC.2019.2903254.
42. Mo, T.; Lau, K.-T.; Li, Y.; Poon, C.-k.; Wu, Y.; Chu, P.K.; Luo, Y. Commercialization of Electric Vehicles in Hong Kong. *Energies* **2022**, *15*, 942. https://doi.org/10.3390/en15030942
43. Garg, S.; Mehrotra, D.; Pandey, H.M.; Pandey, S. Accessible review of internet of vehicle models for intelligent transportation and research gaps for potential future directions. *Peer-to-Peer Networking and Applications* **2021**, *14*, 978–1005. https://doi.org/10.1007/s12083-020-01054-6
44. Sakai, K. Japan perspective. In: Smart Sensing for Traffic Monitoring. Ozaki, N., Ed., The Institution of Engineering and Technology, Herts, UK 2021.
45. Ishikawa, H.; Yamauchi, Y,; Mizouchi, K. Vehicle detection at intersection by LIDAR system. In: Smart Sensing for Traffic Monitoring. Ozaki, N., Ed., The Institution of Engineering and Technology, Herts, UK 2021.
46. Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J.W. Connected vehicles: Solutions and challenges. *IEEE Internet Things J.* **2014**, 1(4), 289–299. https://doi.org/10.1109/JIOT.2014.2327587
47. Sadiku, M.N.O.; Tembely, M.; Musa, S.M. Internet of Vehicles: An Introduction. *International Journals of Advanced Research in Computer Science and Software Engineering* **2018**, *8* (1), 11–13. http://dx.doi.org/10.23956/ijarcsse.v8i1.512
48. Fadhil, J.A.; Sarhan, Q.I. Internet of Vehicles (IoV): A Survey of Challenges and Solutions. In 2020 21st International Arab Conference on Information Technology (ACIT), Muscat, Oman, 28-30 November 2020; pp. 1-10. doi: 10.1109/ACIT50332.2020.9300095.
49. Alam, K.M.; Saini, M.; El Saddik, A.E. Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access* **2015**, *3*, 343–357. DOI: 10.1109/ACCESS.2015.2416657
50. Wu, L.; Zhang, R.; Li, Q.; Ma, C.; Shi, X. A mobile edge computing-based applications execution framework for Internet of Vehicles. *Front. Comput. Sci.* **2022a**, *16*(*5*), 165506 https://doi.org/10.1007/s11704-021-0425-6
51. Richter, A.; Löwner, M.O.; Ebendt, R.; Scholz, M. Towards an integrated urban development considering novel intelligent transportation systems: Urban Development Considering Novel Transport. *Technol. Forecast. Soc. Change* **2020**, *155*, 119970.
52. Internet of Vehicles (IoV). Available online: https://www.techtarget.com/whatis/definition/Internet-of-Vehicles (accessed on 2 December 2020).
53. Chen, C.; Quan, S. Review Article A Summary of Security Techniques-Based Blockchain in IoV. *Security and Communication Networks* **2022**, 8689651. https://doi.org/10.1155/2022/8689651
54. Latif, M.B.; Liu, F.; Liu, K. A TDMA-Based MAC Protocol for Mitigating Mobility-Caused Packet Collisions in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 643. https://doi.org/10.3390/s22020643
55. Huang, J.; Xu, C.; Ji, Z.; Xiao, S.; Liu, T.; Ma, N.; Zhou, Q. Research Article AFLPC: An Asynchronous Federated Learning Privacy-Preserving Computing Model Applied to 5G-V2X. *Security and Communication Networks* **2022**, 9334943. https://doi.org/10.1155/2022/9334943
56. Wu, H.; Liu, Q.; Liu, Q.; Zhang, Y.; Yang, Z. An edge-assisted cloud framework using a residual concatenate FCN approach to beam correction in the internet of weather radars. *World Wide Web* **2022b**. https://doi.org/10.1007/s11280-021-00988-y
57. Yin, D.; Gong, B. Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles. *Wireless Communications and Mobile Computing* **2022**, 3537771. https://doi.org/10.1155/2022/3537771
58. Tomar, A.; Tripathi, S. BCAV: Blockchain-based certificateless authentication system for vehicular network. *Peer-to-Peer Networking and Applications* **2022**, *15*, 1733–1756. https://doi.org/10.1007/s12083-022-01319-
59. Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, N. Blockchain for IoV in 6G environment: review solutions and challenges. *Cluster Computing* **2021**. https://doi.org/10.1007/s10586-021-03492-0
60. Liu, Y.; Liu, J.; Liu, T.; He, X. BSS-ITS: Blockchain Scaling Scheme with Sharding for Intelligent Transportation System. Scale Blockchain for Better Data Exchange and Storage with Full Sharding for Intelligent Transportation System. Proceedings of ICBTA 2021, 17–19 December 2021, Xi’an, China; 128–134.
61. Evariste, T.; Rwigema, J.; Datta, R. Design and Deployment of Vehicular Internet of Things for Smart City Applications. *Sustainability* **2022**, *14*, 176. https://doi.org/10.3390/su14010176
62. Kakkavas, G.; Diamanti, M.; Stamou, A.; Karyotis, V.; Bouali, F.; Pinola, J.; Apilo, O.; Papavassiliou, S.; Moessner, K.; Design, Development, and Evaluation of 5G-Enabled Vehicular Services: The 5G-HEART Perspective. *Sensors* **2022**, *22*, 426. https://doi.org/10.3390/s22020426
63. Xu, W.; Li, N.; Liang, W.; Liu, H. Research Article Dissipation Characteristics of Vehicle Queue in V2X Environment Based on Improved Car-Following Model. *Mathematical Problems in Engineering* **2022**, 8281919. https://doi.org/10.1155/2022/8281919
64. Shiny, G.S.; Kumar, B.M. E2IA-HWSN: Energy Efficient Dual Intelligent Agents based Data Gathering and Emergency Event Delivery in Heterogeneous WSN Enabled IoT. *Wireless Personal Communications* **2022**, *122*, 379–408. https://doi.org/10.1007/s11277-021-08904-3
65. Ullah, S.; Khan, M.A.; Ahmad, J.; Jamal, S.S.; e Huma, Z.; Hassan, M.T.; Pitropakis, N.; Arshad; Buchanan, W.J. HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles. *Sensors* **2022**, *22*, 1340. https://doi.org/10.3390/s22041340
66. Smida, K.; Tounsi, H.; Frikha, M. Intelligent and resizable control plane for software defined vehicular network: a deep reinforcement learning approach. *Telecommunication Systems* **2022**, *79*, 163–180. https://doi.org/10.1007/s11235-021-00838-2
67. Wang, Y.; Wang, X.; Huang, Z.; Li, W.; Xu, S. Joint optimization of dynamic resource allocation and packet scheduling for virtual switches in cognitive internet of vehicles. *EURASIP Journal on Advances in Signal Processing* **2022a**, *32*. https://doi.org/10.1186/s13634-022-00862-7
68. Pachala, S.; Rupa, C.; Sumalatha, L. l−PEES-IMP: lightweight proxy re-encryption-based identity management protocol for enhancing privacy over multi-cloud environment. *Automated Software Engineering* **2022**, *29* (*4*). https://doi.org/10.1007/s10515-021-00299-6
69. Khan, S.; Shah, I.A.; Tairan, N.; Shah, H.; Nadeem, M.F. Optimal Resource Allocation in Fog Computing for Healthcare Applications. *Computers, Materials & Continua* **2022**, *71* (*3*), 6147–6163. https://doi.org/10.32604/cmc.2022.023234
70. Yuan, Z.; Wu, T.; Wang, Q.; Yang Y.; Li, L.; Zhang, L. T 3 OMVP: A Transformer-Based Time and Team Reinforcement Learning Scheme for Observation-Constrained MultiVehicle Pursuit in Urban Area. *Electronics* **2022**, *11*, 1339. https://doi.org/10.3390/electronics11091339
71. Bhabani, B.; Mahapatro, J. ReUse: Reliable and efficient RSU-enabled relay vehicle selection using harmony search and EDAS for message dissemination in VANETs. Ad Hoc *Networks* **2022**, *137*, 102985. https://doi.org/10.1016/j.adhoc.2022.102985.
72. Zhang, L.; Zhou, W.; Xia, J.; Ou, J. DQN-based mobile edge computing for smart Internet of vehicle. *EURASIP Journal on Advances in Signal Processing* **2022**, *45*. https://doi.org/10.1186/s13634-022-00876-1
73. You, K.; Peng, G.; Ding, L.; Dou, Q.; Wu, Z.; Zhou, C. Smart T-box of unmanned earthwork machinery for Internet of Vehicles. *Automation in Construction* **2022**, *144*, 104589. https://doi.org/10.1016/j.autcon.2022.104589.
74. Sellami, B.; Hakiri, A.; Yahiac, S.B. Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network. *Future Generation Computer Systems* **2022**, *137*, 363–379. https://doi.org/10.1016/j.future.2022.07.024.
75. Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, R. Blockchain for IoV in 6G environment: review solutions and challenges. *Cluster Computing* **2022**, *25*, 1927–1955. https://doi.org/10.1007/s10586-021-03492-0.
76. Peng, H.; Dong, L.; Sun, Y.; Jiang, Y. Analysis of Marketing Prediction Model Based on Genetic Neural Network: Taking Clothing Marketing as an Example. *Journal of Mathematics* **2022**, 8743568. https://doi.org/10.1155/2022/8743568
77. Jamalzadeh, M.; Maadani, M.; Mahdavi, M. EC-MOPSO: an edge computing-assisted hybrid cluster and MOPSO-based routing protocol for the Internet of Vehicles. *Annals of Telecommunications* **2022**. https://doi.org/10.1007/s12243-021-00892-6
78. Li, Q.; Wu, H.; Wu, X.; Zhao, N.; Dong, L. A Road Truncation-Based Location Privacy-Preserving Method against Side-Weight Inference Attack. *Appl. Sci.* **2022a**, *12*, 1107. https://doi.org/10.3390/app12031107
79. Hemavathi; Akhila, S.R.; Alotaibi, Y.; Khalaf, O.I.; Alghamdi, S. Authentication and Resource Allocation Strategies during Handoff for 5G IoVs Using Deep Learning. *Energies* **2022**, *15*, 2006. https://doi.org/10.3390/en15062006
80. Gurumoorthi, E.; Ayyasamy, A. Performance analysis of Geocast based location aided routing using Cache agent in VANET. *Int. J. Inf. Technol.* 2022, 14(1), 125–134. https://doi.org/10.1007/s41870-019-00410-x
81. Zhang, L.; Zhong, W.; Zhang, J.; Lin, Z.; Yang, Z.; Wang, J. mmWave Beam Tracking for V2I Communication Systems Based on Spectrum Environment Awareness. *Symmetry* **2022**, *14*, 677. https://doi.org/10.3390/sym14040677
82. Wang, M.; Chen, T.; Du, F.; Wang, J.; Yin, G.; Zhang, Y. Research on adaptive beacon message transmission power in VANETs. *Journal of Ambient Intelligence and Humanized Computing* **2022b**, *13*, 1307–1319. https://doi.org/10.1007/s12652-020-02575-x
83. Chen, X.; Jin, Z.; Zhang, Q.; Li, P.; Zhang, S.; Sun, J.; Tian, X.; Wang, Y.; Zhang, J. Research on Automatic Driving Simulation Test System Based on Digital Twin. *Journal of Physics: Conference Series* **2022**, *2170*, 012039. https://doi.org/10.1088/1742-6596/2170/1/012039
84. Khasawneh, A.M.; Helou, M.A.; Khatri, A.; Aggarwal, G.; Kaiwartya, O.; Altalhi, M.; Abu-ulbeh, W.; AlShboul, R. Service-Centric Heterogeneous Vehicular Network Modeling for Connected Traffic Environments. *Sensors* **2022**, *22*, 1247. https://doi.org/10.3390/s22031247
85. González-Saavedra, J.F.; Figueroa, M.; Céspedes, S.; Montejo-Sánchez, S. Survey of Cooperative Advanced Driver Assistance Systems: From a Holistic and Systemic Vision. *Sensors* **2022**, *22*, 3040. https://doi.org/10.3390/s22083040
86. Zhu, C.; Ye, D.; Zhu, T.; Zhou, W. Time-optimal and privacy preserving route planning for carpool policy. *World Wide Web* **2022**. https://doi.org/10.1007/s11280-022-01026-1
87. Xie, H.; Zhu, J.; Duan, H. Research Article Analysis of the Relationship between the Density and Lane-Changing Behavior of Circular Multilane Urban Expressway in Mixed Traffic. *Journal of Advanced Transportation* **2022**, 4499477. https://doi.org/10.1155/2022/4499477
88. Dhanare, R.; Nagwanshi, K.K.; Varma, S. Enhancing the Route Optimization Using Hybrid MAF Optimization Algorithm for the Internet of Vehicle. *Wireless Personal Communications* **2022**. https://doi.org/10.1007/s11277-022-09629-7
89. Guerna, A.; Bitam, S.; Calafate, C.T. Roadside Unit Deployment in Internet of Vehicles Systems: A Survey. *Sensors* **2022**, *22*, 3190. https://doi.org/10.3390/s22093190
90. Wang, L.; Li, H.; Guo, M.; Chen, Y. The Effects of Dynamic Complexity on Drivers’ Secondary Task Scanning Behavior under a Car-Following Scenario. *Int. J. Environ. Res. Public Health* **2022c**, *19*, 1881. https://doi.org/10.3390/ijerph19031881
91. Bustamante-Bello, R.; García-Barba, A.; Arce-Saenz, L.A.; Curiel-Ramirez, L.A.; Izquierdo-Reyes, J.; Ramirez-Mendoza, R.A. Visualizing Street Pavement Anomalies through Fog Computing V2I Networks and Machine Learning. *Sensors* **2022**, *22*, 456. https://doi.org/10.3390/s22020456
92. Lu, Y.; Wang, X.; Yi, B.; Huang, M. The reliable routing for software-defined vehicular networks towards beyond 5G. *Peer-to-Peer Networking and Applications* **2022**, *15*, 134–148. https://doi.org/10.1007/s12083-021-01231-1
93. Dai, F.; Liu, G.; Mo, Q.; Xu, W.H.; Huang B. Task offloading for vehicular edge computing with edge-cloud cooperation. *World Wide Web* **2022**. https://doi.org/10.1007/s11280-022-01011-8
94. Seng, K.P.; Ang, L.M.; Ngharamike, E. Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks *International Journal of Distributed Sensor Networks* **2022**, *18*(3). https://doi.org/10.1177/15501477211062835
95. Mir, M.; Yaghoobi, M.; Khairabadi, M. A new approach to energy-aware routing in the Internet of Things using improved Grasshopper Metaheuristic Algorithm with Chaos theory and Fuzzy Logic. *Multimedia Tools and Applications* **2022**. https://doi.org/10.1007/s11042-021-11841-9
96. Khezri, E.; Zeinali, E.; Sargolzaey, H. A Novel Highway Routing Protocol in Vehicular Ad Hoc Networks Using VMaSC-LTE and DBA-MAC Protocols. *Wireless Communications and Mobile* *Computing* **2022**, 1680507. https://doi.org/10.1155/2022/1680507
97. Safara, F.; Souri, A.; Baker, T.; Al Ridhawi, I.; Aloqaily, M. A priority-based energy-efficient routing method for IoT systems. *Journal of Supercomputing* **2020**, *76*, 8609–8626. https://doi.org/10.1007/s11227-020-03147-8
98. Li, H.; Ou, D.; Rasheed, I.; Tu, M. Research Article A Software-Defined Networking Roadside Unit Cloud Resource Management Framework for Vehicle Ad Hoc Networks. *Journal of Advanced Transportation* **2022b**, 5918128. https://doi.org/10.1155/2022/5918128
99. Guan, Z.; Wang, Y.; He, M. Deep Reinforcement Learning-Based Spectrum Allocation Algorithm in Internet of Vehicles Discriminating Services. *Appl. Sci.* **2022**, *12*, 1764. https://doi.org/10.3390/app12031764
100. Pereira, P.; Melo, C.; Araujo, J.; Dantas, J.; Santos, V.; Maciel, P. Availability model for edge-fog-cloud continuum: an evaluation of an end-to-end infrastructure of intelligent traffic management service. *The Journal of Supercomputing* **2022**, *78*, 4421–4448. https://doi.org/10.1007/s11227-021-04033-7
101. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.B.M.; Habib A.K.M.A.; Mohd Aman, A.H.; Hossain, Md. A. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wireless Communications and Mobile Computing* **2022**, 9065768. https://doi.org/10.1155/2022/9065768
102. Zhu, Y.; Li, X.; Liu, Q.; Li, Q.; Xu. Y. A comprehensive review of energy management strategies for hybrid electric vehicles. *Mechanical Sciences* **2022**, *13*, 147–188. https://doi.org/10.5194/ms-13-147-2022
103. Alsaawy, Y.; Alkhodre, A.; Abi Sen, A.; Alshanqiti, A.; Bhat, W.A.; Bahbouh, N.M. A Comprehensive and Effective Framework for Traffic Congestion Problem Based on the Integration of IoT and Data Analytics. *Appl. Sci.* **2022**, *12*, 2043. https://doi.org/10.3390/app12042043
104. Ang, L.M.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for smart cities: Applications, architecture, and challenges. *IEEE Access* **2018**, *7*, 6473–6492. https://doi.org/10.1109/ACCESS.2018.2887076.
105. Salih, K.O.M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A Comprehensive Survey on the Internet of Things with the Industrial Marketplace. *Sensors* **2022**, *22*, 730. https://doi.org/10.3390/s22030730
106. Tan, L.; Wang, N. Future Internet: The Internet of Things. In Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, ICACTE 2010, Chengdu, China, 20–22 August 2010; pp. V5-376–V5-380. https://doi.org/10.1109/ICACTE.2010.5579543
107. Kopelias, P.; Demiridi, E.; Vogiatzis, K.; Skabardonis, A.; Zafiropoulou, V. Connected & autonomous vehicles - Environmental impacts - A review. *Science of the Total Environment* **2020**, *712*, 135237. https://doi.org/10.1016/j.scitotenv.2019.135237
108. Sharma, N.; Habibullah, P.S. A Review of IoT Technology for the Connected Autonomous Vehicles Ecosystem. *Trends in Sciences* **2022**, *19*(7), 3072. https://doi.org/10.48048/tis.2022.3072
109. Butt, T.A.; Iqbal, R.; Shah, S.C.; Umar, T. Social Internet of Vehicles: Architecture and enabling technologies. *Computers and Electrical Engineering* **2018**, *69*, 68–84. https://doi.org/10.1016/j.compeleceng.2018.05.023.
110. Zhang, L.; Zhao, Z.; Wu, Q.; Zhao, H.; Xu, H.; Wu, X. Energy-aware dynamic resource allocation in UAV assisted mobile edge computing over social internet of vehicles. *IEEE Access* **2018**, *6*, 8478172, 56700–56715. https://doi.org/10.1109/ACCESS.2018.2872753
111. Silva, R.; Iqbal, R. Ethical Implications of Social Internet of Vehicles Systems. IEEE Internet of Things Journal **2019**, *6* (1), 517–531. https://doi.org/10.1109/JIOT.2018.2841969.
112. Javaid, U.; Sikdar, B. A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles. *IEEE Transactions on Vehicular Technology* **2021**, *70* (5), 9356256, 4022–4036. https://doi.org/10.1109/TVT.2021.3060002
113. Zhao, Y.; Liu, W.; Li, B.; Zhou, X.; Ning, Z.; Qiu, T.; Atiquzzaman, M. Entity and Sociality Trust-Aware Model for Content Distribution in Social Internet of Vehicles. *IEEE Transactions on Vehicular Technology* **2022a**, *1*. https://doi.org/10.1109/TVT.2022.3196671
114. Howard, M.; Sparrow, R. When human beings are like drunk robots: Driverless vehicles, ethics, and the future of transport. *Transp. Res. C Emerg. Technol.* **2017**, *80*, 206–215. https://doi.org/10.1016/j.trc.2017.04.014
115. Maglaras, L.A.; Al-Bayatti, A.H.; He, Y.; Wagner, I.; Janicke, H. Social Internet of Vehicles for Smart Cities. J. Sens. Actuator Netw. **2016**, 5, 3. https://doi.org/10.3390/jsan5010003
116. Butt, T.A.; Iqbal, R.; Salah, K.; Aloqaily, M.; Jararweh, Y. Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions. *IEEE Access* **2019**, *7*, 8735700, 79694–79713. https://doi.org/10.1109/ACCESS.2019.2922236
117. Loscri, V.; Manzoni, O.; Nitti, M.; Ruggeri, G.; Vegni, A.M. A social internet of vehicles sharing SIoT relationships. In MobiHoc 2019: Twentieth International Symposium on Mobile Ad Hoc Networking; Catania, Italy, 2–5 July 2019. Association for Computing Machinery: New York, NY, USA, 2019. https://doi.org/10.1145/1122445.1122456
118. Eftekhari, S.A.; Nikooghadam, M.; Rafighi, M. Robust session key generation protocol for social internet of vehicles with enhanced security provision. *Journal of Supercomputing* **2021**, *77* (3), 2511–2544. https://doi.org/10.1007/s11227-020-03363-2
119. Khan, S.; Zhu, L.; Yu, X.; Zhang, Z.; Rahim, M.A.; Khan, M.; Du, X.; Guizani, M. Accountable credential management system for vehicular communication. *Vehicular Communications* **2020**, *25*, 100279. https://doi.org/10.1016/j.vehcom.2020.100279.
120. Li, Y., Tao, X., Zhang, X., Xu, J., Wang, Y., Xia, W. A DAG-based reputation mechanism for preventing peer disclosure in SIoV. *IEEE Internet of Things Journal* **2022**. https://doi.org/10.1109/JIOT.2022.3189108
121. García-Magariño, I.; Sendra, S.; Lacuesta, R.; Lloret, J. Security in vehicles with iot by prioritization rules, vehicle certificates and trust management. *IEEE Int. Things J*. **2019**, *6* (4), 5927–5934. https://doi.org/10.1109/JIOT.2018.2871255.
122. Lin, K.; Li, C.; Fortino, G.; Rodrigues, J.J. Vehicle route selection based on game evolution in social internet of vehicles. *IEEE Int. Things J.* **2018**, *5* (4), 2423–2430. https://doi.org/10.1109/JIOT.2018.2844215.
123. Tang, C.; Wei, X.; Liu, C.; Jiang, H.; Wu, H.; Li, Q. UAV-enabled social internet of vehicles: Roles, security issues and use cases. *Communications in Computer and Information Science* **2020**, *153*, 163, 1298 CCIS. 10.1007/978-981-15-9031-3\_14.
124. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (SIoT) when social networks meet the internet of things: concept, architecture and network characterization. *Comput. Netw.* **2012**, *56* (16), 3594–3608. https://doi.org/10.1016/j.comnet.2012.07.010.
125. Hussain, R.; Kim, D.; Son, J.; Lee, J.; Kerrache, C.A.; Benslimane, A.; Oh, H. Secure and Privacy-Aware Incentives-Based Witness Service in Social Internet of Vehicles Clouds. *IEEE Internet of Things Journal* **2018**, *5* (4), 8383974, 2441–2448. https://doi.org/10.1109/JIOT.2018.2847249
126. Jain, B.; Brar, G.; Malhotra, J.; Rani, S.; Ahmed, S.H. A cross layer protocol for traffic management in social internet of vehicles. *Future Gener. Comput. Syst.* **2018**, *82*, 707–714. https://doi.org/10.1016/j.future.2017.11.019.
127. Raza, N.; Jabbar, S.; Han, J.; Han, K. Social Vehicle-To-Everything (V2X) communication model for Intelligent Transportation Systems based on 5G scenario. *ACM International Conference Proceeding Series* **2018**, *54*. https://doi.org/10.1145/3231053.3231120
128. Zualkernan, I.A.; Aloul, F.; Al Qasimi, S.; AlShamsi, A.; Al Marashda, M.; Ahli, A. DigiMesh-based Social Internet of Vehicles (SIoV) for Driver Safety. 2018 International Symposium in Sensing and Instrumentation in IoT Era, ISSI 2018; Shanghai, Chuna, 6-7 September 2018; IEEE: Piscataway, NJ, USA; 8538167. https://doi.org/10.1109/ISSI.2018.8538167
129. Wang, T.; Hussain, A.; Zhang, L.; Zhao, C. Collaborative Edge Computing for Social Internet of Vehicles to Alleviate Traffic Congestion. *IEEE Transactions on Computational Social Systems* **2022d**, *9* (1), 184–196. https://doi.org/10.1109/TCSS.2021.3074038
130. Roopa, M.S.; Ayesha Siddiq, S.; Buyya, R.; Venugopal, K.R.; Iyengar, S.S.; Patnaik, L.M. Dynamic traffic congestion management in Social Internet of Vehicles (SIoV). *Internet of Things (Netherlands)* **2021**, *16*, 100311. https://doi.org 10.1016/j.iot.2020.100311.
131. Tang, C.; Wu, H. Reputation-based service provisioning for vehicular fog computing. *Journal of Systems Architecture* **2022**, *131*, 102735. https://doi.org/10.1016/j.sysarc.2022.102735.
132. Jennath, H.S.; Asharaf, S. Reputation management in vehicular network using blockchain. *Peer-to-Peer Networking and Applications* ***2022***, *15* (2), 901–920. https://doi.org/10.1007/s12083-021-01249-5
133. Ochoa-Zambrano, J.; Garbajosa, J. Social Internet of Things: Architectural Approaches and Challenges. Actas de las 24th Jornadas de Ingenieria del Software y Bases de Datos, JISBD 2019; Caceres, Spain, 2–4 September 2019.
134. Kehal, M.; Zhang, Z. Social internet of vehicles: an epistemological and systematic perspective. *Library Hi Tech* **2020**, *38* (1), 221–231. https://doi.org/10.1108/LHT-12-2017-0259
135. Kerrache, C.A.; Lagraa, N.; Hussain, R.; Ahmed, S.H.; Benslimane, A.; Calafate, C.T.; Cano, J.-C.; Vegni, A.M. TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles. *IEEE Internet of Things Journal* **2019**, *6* (4), 8527532, 5870–5877. https://doi.org/10.1109/JIOT.2018.2880332
136. Xia, Z.; Mao, X.; Gu, K.; Jia, W.J. Dual-Mode Data Forwarding Scheme Based on Interest Tags for Fog Computing-based SIoVs. *IEEE Transactions on Network and Service Management* **2022**., *19*(3), 2780–2797. https://doi.org/10.1109/TNSM.2022.3161539
137. Xia, Z.; Mao, X.; Gu, K.; Jia, W. Two-Dimensional Behavior-Marker-Based Data Forwarding Incentive Scheme for Fog-Computing-Based SIoVs. *IEEE Transactions on Computational Social Systems* **2022**, *9* (5), 1406–1418. https://doi.org/10.1109/TCSS.2021.3129898
138. Ruan, Z.; Liang, W.; Luo, H.; Yan, H. A novel data sharing mechanism via cloud-based dynamic audit for social internet of vehicles. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **2015**, *9502*, 78–88. https://doi.org/10.1007/978-3-319-27293-1\_8
139. Nitti, M.; Girau, R.; Floris, A.; Atzori, L. On adding the social dimension to the Internet of Vehicles: Friendship and middleware. 2014 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2014; Chişinău, Moldova, 27-30 May 2014, 6849025; pp. 134–138. https://doi.org 10.1109/BlackSeaCom.2014.6849025
140. Wang, X.; Ning, Z.; Hu, X.; Ngai, E.C.-H.; Wang, L.; Hu, B.; Kwok, R.Y.K. A City-Wide Real-Time Traffic Management System: Enabling Crowdsensing in Social Internet of Vehicles. *IEEE Communications Magazine* **2018**, *56* (9), 8466350, 19–25. https://doi.org/10.1109/MCOM.2018.1701065
141. Zhao, P.-C.; Huang, Y.-H.; Zhang, D.-X.; Xing, L.; Wu, H.-H.; Gao, J.-P. CCP-federated deep learning based on user trust chain in social IoV. Wireless Networks 2021b. https://doi.org/10.1007/s11276-021-02870-1
142. Li, Y.; Cao, B.; Peng, M; Zhang, L.; Zhang, L.; Feng, D.; Yu, J. Direct Acyclic Graph-Based Ledger for Internet of Things: Performance and Security Analysis. *IEEE/ACM Transactions on Networking* **2020**, *28*(4),1643-1656. doi: 10.1109/TNET.2020.2991994.00
143. Zhao, P.; Huang, Y.; Gao, J.; Xing, L.; Wu, H.; Ma, H. Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV. *IEEE Sensors Journal* **2022**, *22* (7), 7385–7398. https://doi.org/10.1109/JSEN.2022.3153338
144. Kong, X.; Gao, H.; Shen, G.; Duan, G.; Das, S.K. FedVCP: A Federated-Learning-Based Cooperative Positioning Scheme for Social Internet of Vehicles. *IEEE Transactions on Computational Social Systems* **2022**, *9* (1), 197–206. https://doi.org/1010.1109/TCSS.2021.3062053
145. Jia, X.; Xing, L.; Gao, J.; Wu, H. A Survey of Location Privacy Preservation in Social Internet of Vehicles. *IEEE Access* **2020**, *8*, 9248987, 201966–201984. https://doi.org/10.1109/ACCESS.2020.3036044
146. Xing, L.; Jia, X.; Gao, J.; Wu, H. A Location Privacy Protection Algorithm Based on Double K-Anonymity in the Social Internet of Vehicles. *IEEE Communications Letters* **2021**, *25* (10), 3199–3203. https://doi.org/10.1109/LCOMM.2021.3072671
147. Li, Z.; Miao, Q.; Chaudhry, S.A.; Chen, C.-M. A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles. *International Journal of Distributed Sensor Networks* **2022**, *18* (6). https://doi.org/1010.1177/15501329221104332
148. Wu, T.Y.; Guo, X.; Yang, L.; Meng, Q.; Chen, C.-M. A lightweight authenticated key agreement protocol using fog nodes in social Internet of vehicles. *Mob. Inf. Syst.* **2021**; *2021*, 3277113. https://doi.org/10.1155/2021/3277113
149. Chen, P.-Y.; Cheng, S.-M.; Sung, M.-H. Analysis of Data Dissemination and Control in Social Internet of Vehicles*. IEEE Internet of Things* Journal **2018**, *5* (4), 8383978, 2466–2477. https://doi.org/10.1109/JIOT.2018.2846722
150. Kumar, N.; Chaudhry, R.; Kaiwartya, O.; Kumar, N.; Ahmed, S.H. Green Computing in Software Defined Social Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems* **2021**, *22* (6), 9234040, 3644–3653. https://doi.org/10.1109/TITS.2020.3028695
151. Kumar, T.A.; Rajmohan, R.; Julie, E.G.; Robinson, Y.H.; Vimal, S.; Kadry, S. Reinforced resource management in vehicular fog computing using deep beacon power control protocol. *International Journal of Web and Grid Services* **2021**, *17* (4), 371–388. https://doi.org/10.1504/IJWGS.2021.118404
152. Gulati, A.; Aujla, G.S.; Chaudhary, R.; Kumar, N.; Obaidat, M.S.; Benslimane, A. DiLSe: Lattice-Based Secure and Dependable Data Dissemination Scheme for Social Internet of Vehicles. *IEEE Transactions on Dependable and Secure Computing* **2021**, *18* (6), 2520–2534. https://doi.org/10.1109/TDSC.2019.2953841
153. Liu, Y.; Xiong, Z.; Hu, Q.; Niyato, D.; Zhang, J.; Miao, C.; Leung, C.; Tian, Z. VRepChain: A Decentralized and Privacy-preserving Reputation System for Social Internet of Vehicles Based on Blockchain. *IEEE Transactions on Vehicular Technology* **2022**, *1* (12). https://doi.org/10.1109/TVT.2022.3198004
154. Bao, Y.; Qiu, W.; Cheng, X.; Sun, J. Fine-Grained Data Sharing with Enhanced Privacy Protection and Dynamic Users Group Service for the IoV. *IEEE Transactions on Intelligent Transportation Systems* **2022**. https://doi.org/10.1109/tits.2022.3187980
155. Al Zamil, M. GH.; Samarah, S.; Rawashdeh, M.; Hossain, M. S.; Alhamid, M. F.; Guizani, M.; Alnusair, A. False-Alarm Detection in the Fog-Based Internet of Connected Vehicles. *IEEE Transactions on Vehicular Technology* **2019**, *68*(7), 7035–7044. https://doi.org/10.1109/tvt.2019.2917288
156. Qian, Y.; Chen, M.; Chen, J.; Hossain, M.S.; Alamri, A. Secure enforcement in cognitive Internet of Vehicles. *IEEE Internet Things Journal* **2018,** *5*(2), 1242–1250.
157. Alotaibi, J.; Alazzawi, L. PPIoV: A privacy preserving-based framework for IoV-fog environment using federated learning and blockchain. 2022 IEEE World AI IoT Congress, AIIoT 2022; Seattle, USA, 6–9 June 2022; pp. 597-603. https://doi.org/10.1109/AIIoT54504.2022.9817205
158. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Information Processing and Management* **2021***, 58*(3) https://doi.org/10.1016/j.ipm.2021.102511
159. Wu, X.; Xu, X.; Bilal, M. Towards privacy protection composition framework on internet of vehicles. *IEEE Consumer Electronics Magazine 2021,* 11(6), 32–38. https://doi.org/10.1109/MCE.2021.3092303
160. Kim, S.-K. Enhanced IoV Security Network by Using Blockchain Governance Game. *Mathematics* **2021**, *9*, 109. https://doi.org/10.3390/math9020109
161. Abbas, S.; Talib, M. A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.-H. Blockchain-Based Authentication in Internet of Vehicles: A Survey. *Sensors* **2021**, *21*(23), 7927. https://doi.org/10.3390/s21237927
162. Feng, X.; Li, C.; Chen, D.; Tang, J. A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 305–314. https://doi.org/10.1007/s12083-016-0431-x
163. Xie, Y.; Wu, L.; Shen, J.; Alelaiwi, A. EIAS-CP: New efficient identity-based authentication scheme with conditional privacy preserving for VANETs. *Telecommun. Syst.* **2017**, *65*, 229–240. https://doi.org/10.1007/s11235-016-0222-y
164. Biswas, S.; Misic, J. A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs. *IEEE Trans. Veh. Technol*. **2013**, *62*, 2182–2192. https://doi.org/10.1109/TVT.2013.2238566
165. Sahraoui, Y.; Kerrache, C. A.; Korichi, A.; Vegni, A.M.; Amadeo, M. LearnPhi: A real-time learning model for early prediction of phishing attacks in IoV. Proceedings - IEEE Consumer Communications and Networking Conference, CCNC 2022, Virtual Conference, 8–11 January 2022; pp. 252-255. https://doi.org/10.1109/CCNC49033.2022.9700545
166. Kumar, A.; Das, D. SIoVChain: Efficient and secure blockchain based internet of vehicles (IoV). 23rd International Conference on Distributed Computing and Networking, Association for Computing Machinery International Conference Proceeding Series, Delhi, AA, India; Association for Computing Machinery: New York, NY, USA; pp. 284–289. https://doi.org/10.1145/3491003.3494123
167. Li, F.; Li, X.; Fu, Y.; Zhao, P.; Liu, S. A secure and privacy preserving incentive mechanism for vehicular crowdsensing with data quality assurance. IEEE Vehicular Technology Conference 2021; virtual conference, 27 September – 28 October 2021.https://doi.org/10.1109/VTC2021-Fall52928.2021.9625317
168. Bai, X.; Chen, S.; Shi, Y.; Liang, C.; Lv, X. Blockchain-based authentication and proof-of-reputation mechanism for trust data sharing in internet of vehicles. *Ad-Hoc and Sensor Wireless Networks* **2022**, *53*(1-2), 85–113. https://doi.org/10.32908/ahswn.v53.8647
169. Hou, B.; Zhu, H.; Xin, Y.; Wang, J.; Yang, Y. MPoR: A modified consensus for blockchain-based internet of vehicles. *Wireless Communications and Mobile Computing* **2022**, 1644851. https://doi.org/10.1155/2022/1644851
170. Zhang, J.; Wu, M. Blockchain-based authentication with optional privacy preservation for internet of vehicles. *Mathematical Problems in Engineering* **2021**, 9954599. https://doi.org/10.1155/2021/9954599
171. Ma, Z.; Wang, L.; Zhao, W. Blockchain-driven trusted data sharing with privacy protection in IoT sensor network. *IEEE Sensors Journal* **2021**, *21*(22), 25472–25479. https://doi.org/10.1109/JSEN.2020.3046752
172. Liu, J.; Zhang, G.; Sun, R.; Du, X.; Guizani, M. A blockchain-based conditional privacy-preserving traffic data sharing in cloud. IEEE International Conference on Communications 2020, virtual conference, 7-11 June 2020.https://doi.org/10.1109/ICC40277.2020.9148864
173. Firdaus, M.; Rahmadika, S.; Rhee, K. Decentralized trusted data sharing management on internet of vehicle edge computing (iovec) networks using consortium blockchain. *Sensors* **2021**, *21*(7) https://doi.org/10.3390/s21072410
174. Haddaji, A.; Ayed, S.; Chaari, L. Federated Learning with Blockchain Approach for Trust Management in IoV. In: Barolli, L., Hussain, F., Enokido, T., eds.; Advanced Information Networking and Applications. AINA 2022; Lecture Notes in Networks and Systems, vol. 449; Springer, Cham, Switzerland; pp. 411–423. https://doi.org/10.1007/978-3-030-99584-3\_36
175. Shrivastava, A.L.; Dwivedi, R.K. A secure design of the smart vehicular IoT system using blockchain technology. Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development, INDIACom 2022, New Delhi, India, 23-25 March 2022; pp. 616-620. https://doi.org/10.23919/INDIACom54597.2022.9763216
176. Gong, Y.; Feng, H.; Zhang, C. Research on the Development Strategy of the Internet of Vehicles. *Journal of Physics: Conference Series* **2021**, *1907*, 012063. https://doi.org/10.1088/1742-6596/1907/1/012063