Hindawi
Security and Communication Networks
Volume 2022, Article ID 1131479, 19 pages
https://doi.org/10.1155/2022/1131479

Review Article

Architecture, Protocols, and Security in IoV: Taxonomy, Analysis, Challenges, and Solutions

Sulaiman M. Karim,[1] **Adib Habbal**,[1] **Shehzad Ashraf Chaudhry**,[2,3] **and Azeem Irshad**[4]

[1]*Department of Computer Engineering, Faculty of Engineering, Karabuk University, Karabuk, Turkey*
[2]*Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, UAE*
[3]*Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul 34398, Turkey*
[4]*Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan*

Correspondence should be addressed to Azeem Irshad; irshadazeem2@gmail.com

Received 24 June 2022; Revised 5 August 2022; Accepted 9 September 2022; Published 11 October 2022

Academic Editor: David Megias

Internet of Vehicles (IoV) is a multinode network that exchanges information in an open, wireless environment. Various communication activities exist between IoV entities to share important information such as (ID, location, speed, messages, and traffic information), necessary for network operation. As part of intelligent transportation, IoV is considered a hot subject for researchers, because it is still facing many unresolved challenges, especially those concerning security and privacy. The variation of security-privacy threats that can menace the safety, privacy, and lives of vehicle occupants makes security the leading point of interest. The development of communication protocols for autonomous vehicles opens to us new issues to study and enhance the performance of IoV networks in terms of security and privacy. Several works have been reported, proposing many solutions for practical security challenges including a considerable number of survey-review papers published in respectable channels. The main motive of this review paper is to present the latest developments related to IoV security, as well as to address existing limitations. The high frequency of publication on IoV architecture, security, and new solutions leads us to write a compact, comprehensive, and up-to-date review. Inclusion criteria for selected papers include recent publications, number of citations, and impact of the research. In the present survey paper, the IoV architecture model is defined with all related communication types, and security and privacy issues are analyzed and presented with recently proposed solutions in a clear method. Clear classifications of threats, attacks, protocols, and solutions are presented. Moreover, the use of blockchain-based IoV to improve system security is discussed highlighting the most important trends and taxonomies. The paper was written to be a candidate as the first to read on the topic of the IoV security challenge, presenting problems and solutions in a clear, smooth, complete, and integrated manner.

1. Introduction

Nowadays, the rapid development in technology has given rise to a global networking era, consisting of many heterogeneous networks used by a wide range of devices. The Internet of Things (IoT) refers to the whole network infrastructure of those things that deliver different services to consumers. The Internet of Vehicles (IoV) is a term that originated from the IoT as a dynamic network infrastructure connecting vehicles, users, and other smart devices to the Internet. Users are humans involved in the scheme, such as pilots, riders, and even roadside pedestrians. There is an increasing number of vehicles connected to the IoV systems, where every vehicle presents a node in the network [1].

The industrialization of vehicles has become an interesting issue for computer experts as well as mechanical engineers. The fusion of data and communication between technology and cars has transformed conventional vehicles into next-generation intelligent vehicles. This new technology is attracting various interdisciplinary engineers in the manufacturing and deployment processes. IoVs are artificial intelligence (AI)-enabled computer-controlled driverless

vehicles that can take adaptive and effective decisions independently [2]. Vehicles have several number of sensors installed on board, enabling them to collect big environmental data and then process and analyze it with local computing units. Local data storage is also available in vehicles for future use, where the information collected by various vehicles within the vehicular cloud is shared via the IoV network [3]. Depending on the vehicle autonomy, there are two major classes, which are partially and fully automated vehicles. While vehicles with a partial degree of autonomy allow the driver more control and functions during operation, fully automated vehicles are expected to have complete control over all functions.

There are two sources of environmental data that are collected from onboard sensors and those from other vehicles and nearby infrastructure. Data are collected, classified, processed, and used for full or partial automated moreover [4]. A range of technology corporations, automotive companies and suppliers, startups, and academic plans are leading various technological forces to develop the systems needed to make transportation more responsive, accessible, and ultimately safer for all consumers. With technological improvements in external sensing, path planning, vehicle control, and more, innovations around autonomous and highly automated vehicle improvement are finding their way into consumer vehicles in the form of active safety, driver support systems, and short automated driving traits. The statistics show that there happens approximately 8 million accidents per year, which cause 8.3 million injuries or deaths. Similarly, the traffic jams and accidents also cause losses of 90 million of hours costing 2% negative impact on global economy [5]. This calls for the importance of using Intelligent Transportation Systems (ITS). IoV as part of ITS can build a network that will serve a range of functions such as intelligent traffic management, dynamic information services, and intelligent vehicle control, among others [6].

Security is one of the quality of service (QoS) measures that distinguish all IoT systems because of the hard-to-secure Internet used as communications infrastructure [7, 8]. Due to factors such as mobility, human life involvement, and the wide range of security attacks, IoV is known for its exceptional complexity, setting it apart from any other IoT systems in terms of security challenges [9, 10]. The vehicle being mobile can face disconnection from the network, wireless bottlenecks, and security threats in various geographical locations. IoV system deals with user safety directly, and it is the top priority for the system implying a real-time measure. Finally, it is susceptible to increasing attacks due to its connectivity to various parties making it "an easy target" for attacks. Another important issue is identifying de-synchronization apart from several attacks on IoV systems [11]. The main target of this work is to discuss the security challenges and concerns for the IoV by providing a systematic review of threats considered in the new-previous research in the field. The study also proposes solutions to every security challenge by clarifying the most known publications in the IoV security state of the arts.

The article is organized as follows: the basic architecture model of IoV is reviewed in Section 2, attacks on security and privacy are listed in Section 3, the security challenges together with their corresponding antimeasure are presented in Section 4, the opportunity for IoV security using blockchain is given in Section 5, most important survey papers in the field are shown and compared to this paper in Section 6, and Section 7 concludes the article.

1.1. IoV Architecture. Many studies have established a three-layer architecture centered on the integration of various technologies in the IoV milieu. These are sensing, communication, and statistical tools layers [12]. The first layer includes sensor nodes inside the vehicle, which are used to collect local information and detect specific situations of importance such as the vehicle's operating conditions and driving method. The communication layer is the second level, supporting different V2X communication activities. It ensures that current and emerging networks are linked seamlessly via existing communication standards. Layer three includes statistical hardware, storage capacity, processing unit, shaping IoV intelligence and provides big data-based processing capacity. This 3-layer model contains several weaknesses such as lack of consideration for security, incomplete communication selection procedure, limited interaction between driver and passenger, and limited data processing model.

Other architectures have been proposed, but most of them have failed to provide a complete description of the IoV environment [13]. Contreras et al. proposed in [5] a 7-layer, complete, leading model to describe the IoV architecture. These layers from down to top are user vehicle interface, data acquisition, data filtering, communication and reprocessing, control and management, processing, and security management layers. The latter layer is specifically important to provide security measures for the IoV environment. It is a transversal layer having a direct virtual connection with the six other layers. It is responsible for all security functions such as authentication, data integrity, and confidentiality, amongst others.

1.2. IoV Communication Model. IoV facilitates the exchanging of information among cars, road infrastructures, travelers, drivers, sensors and electric actuators, and the Internet using communication protocols such as IEEE802.11p [14]. IoV requires vehicles to be continuously linked to the Internet, creating a network of interconnected vehicles that can provide data for various services such as traffic control and public protection [15]. IoV is treated as an extension of a Vehicle-to-Vehicle (V2V) to a V2X communications network. It is connected in an ad hoc network environment that uses every vehicle in the network as a node, where vehicles can also be connected to the public Internet [16].

V2X is composed of five types of connectivity, which are InterVehicle (Inter-V), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Cloud (V2C) as shown in Figure 1. Inter-V communication is used to monitor the information collected by the vehicle's internal sensors regarding the machine's self-status and nearby environmental data. All the users inside are connected to this communication and data sharing

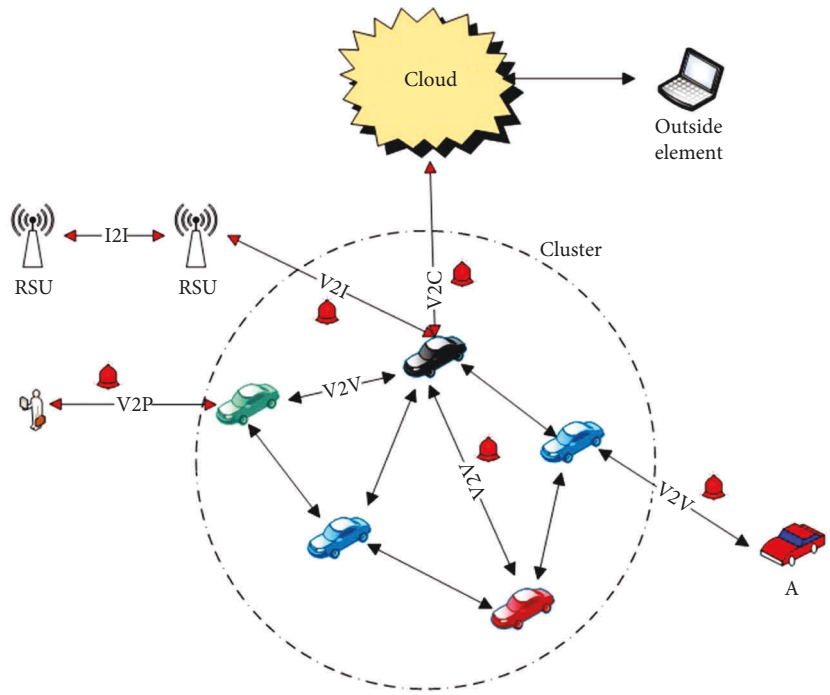

Figure 1: IoV communications.

protocol, which is responsible for good wireless communication between the actors. V2V is a wireless connection between vehicles on a nearby road to obtain information about their location, speed, and other useful data. The V2P connection allows the vehicle to monitor, verify, and communicate with pedestrians and cyclists on the roads to prevent accidents through the awareness of high-risk road users (VRUs) system. There is a continuous exchange of information between vehicle and infrastructure roadside units (RSUs) using V2I, providing services in the wireless communication between the vehicle and the road service provider's data center [17]. Finally, V2C connectivity allows the vehicle to acquire and store data on the cloud and also provides access to the system to obtain additional information through the application program interfaces (APIs).

A complementary communication type can be added to fully describe activities in an IoV system, which is the infrastructure-to-Infrastructure (I2I) communication. The vehicle is not part of the I2I communication path, but it is still part of the network that can impact security as a source of potential attacks. Vehicles are grouped into clusters where V2I, and V2C communication is performed via the cluster head (CH). The adopted clustering architecture contributes to isolating untrusted nodes and then improving IoV security. CH checks cluster-member message validity and sends it to the RSU on behalf of all the vehicles based on ID-based or credential-based authentication. CH is the manager, responsible for all communication inside the cluster, and acts as a gateway to the cluster outside.

1.3. IoV Components. IoV components, such as any IoT-based system, rely on data sensing, processing, communication, decision-making, and information projection. Data sensing is a process performed by many types of sensors including global positioning system (GPS), light detection and ranging (LIDAR), cameras, radar, and electronic control units (ECUs). GPS is the sensing device for locating the vehicle with accurate coordinates using the universal location system. It is a receiver that used received signals from known-location satellites with timing to localize the device with a distinguished precision.

GPS information is evaluated based on received signals which are unavailable or limited in covered areas such as tunnels, representing the major weakness besides its limitations. Although the GPS accuracy is about 10–15 meters, the rapid developments of new sensor technologies such as light detection, LIDAR, and cameras can improve the accuracy of vehicle location [18]. LIDAR is a device used for mapping, localization, and obstacle avoidance, triggered by firing a beam from the vehicle roof surface and shifting the reflection time to measure the exact distance. It is applied to represent high-resolution maps, locating a moving vehicle, and front obstacles detection [19].

To improve the safety of the self-driving car, several cameras, eight or more, are installed around the vehicle, used to mark and track objects, such as pathway following, traffic light detection, and pedestrian detection. They are used to discover, recognize, and track objects in the front, back, and sides of the vehicle. Cameras are usually operating at 60 Hz and, when combined, generate several gigabytes of data flow per second [20]. The radar system performs its usual function of target identification within a certain range and the speed of moving objects. The information produced by the radar shows the distance to the nearest object in front of the vehicle, activating brakes automatically in critical situations challenging vehicle safety. Accordingly, the information collected by radar is applied to generate a real-time

control process without delay. There is short-range and large-range radar in the IoV [21].

Finally, smart driving requirements for IoV impose the necessity of using complicated onboard electronic circuitry, where the ECU is the most considerable, hence the increased complexity of inter-ECUs communications. To fulfill the ultimate target of new service requirements when designing a high-performance, secure, stable, unified, distributed, and scalable IoV system, the following design concepts should be considered [22]:

(i) Invulnerability: even if one or more nodes crash, the computing will resume on the remaining nodes

(ii) Simple to deploy: existing network infrastructure should be used to the maximum extent possible, with the option of adding additional nodes

(iii) Adaptability: the network infrastructure should be able to adapt to evolving conditions and extend its usage to satisfy increasing consumer demands

(iv) Scalability: it necessitates the networks' ability to add/remove equipment to handle the huge data explosion

(v) Safety and security: an essential aim of the IoV architecture is to protect the vehicular network's communications and data protection

(vi) Fault tolerance and high availability: the IoV should be simple to use and reliable

1.4. IoV Protocol. Communication diversity in IoV is achieved through various V2X communication protocols. The main point to secure the IoV environment needs clear comprehension of the occurrence of IoV-related activities. These protocols make a system able to communicate wirelessly within the IoV environment and assist us with the traffic load on a path, filling stations near us, roadside services, and much more [23]. IoV protocols are classified into three classes according to the layer where they are acting. The OSI-ISO seven-layer network model is adopted here because most of the protocols have been invented for networking models in general and not specifically for IoV.

1.4.1. Physical Layer Protocols. The physical layer is analogous to the user interface layer in the IoV architecture. In the design stage of the physical layer, the Doppler frequency shifts and multipath fading that are caused by the vehicles and their movements must be considered. Some of the new invention in this field includes the use of radio waves and infrared for the short-range communication, which is better in performance for broadcasting and line of sight communications. The protocol IEEE 802.11p is based on the standards wireless access of vehicular environment (WAVE). It is widely used for short-range communication between vehicles. It considers all the security concerns so why this protocol is preferred over all the protocols that meet the basic standards of the IEEE-160. The main purpose of the WAVE IEEE 802.11p protocol is to combine the MAC layer and physical to make possible the communication between the vehicles and roadside devices placed at different ranges on-road [24].

(i) MAC layer protocols: IEEE-802.11p is one of the best protocols that enable intervehicular communication with low latency and high reliability. It shares the bandwidth between vehicles by using CSMA and OFDM technology to avoid a collision. Another protocol is the DMAC which is used to increase the rate of reusability of the channels of transmission. It allows for reducing the collisions of antenna direction and improved the performance. ALOHA is also another approach to MAC protocol, where most of the MAC protocols such as VC-MAC and ADHOC MAC, are based on scheduling their transmission. These protocols are preferred over all the protocols working on the ALOHA approach and nominated as an alternative to the Cooperative Communication protocols in the Vehicles Ad Hoc. They are compatible in increasing transmission reusability and throughput and also reduce the collision in transmission between vehicles and roadside devices [5].

(ii) Routing protocols (RP): RPs are part of the network layer, which is analogous to the communication layer in the IoV, 7-layer model [25]. An RP provides the best route from a source node to a destination node according to a cost function such as distance, delay, number of intermediate nodes, and security. It also allows all the nodes on a network to multicommunicate with each other in a specific region using broadcast or geo-cast routing.

A flooding-based algorithm is known for its simplicity compared to others but generates a high overhead, which is negatively reflected on the IoV network performance. It is decreasing communication efficiency, affecting network security, and is not suitable for a large network. Vehicles may contain a dynamic attitude; in this case, maybe they contain the wrong information in their routing tables (RTs), causing many problems and issues in finding the best routes.

There are two types of delay-based routing, delay-sensitive, and delay-tolerant protocols. A delay-sensitive is a protocol that exchanges data as soon as it is possible, whereas the delay-tolerant protocol is the protocol that manages the occurrence of connection failure using a specific mechanism named "Carry and Forward." It is applied to cover large networks but with limited communication. The information-based RPs are topology-based, position-based, map-based, and path-based. The RP that contains the topology and the other related information is called the topology-based routing protocol. The position-based RP is that containing the information about the vehicle's position. The path-based RP provides us the information on the suitable path or the alternative path in case of any problem and trouble. There are two types of targeted-based RPs which are homogenous target-based and heterogeneous-based routing. In homogenous targeted-based RPs, communication within

the same network node is treated, while the communication of nodes based on different path types and networks is considered in a heterogeneous RP [26].

2. Possible Attacks on IoV

Many attacks targeting IoV share the same scenarios with normal IT and various IoT applications. The only difference is the severity and impact of some attacks on the IoV network, which makes it more sensitive and vulnerable than other IT systems. The following are some attacks challenging the IoV environment:

(i) Impersonation attack: attacker could present himself as a legal vehicle to get benefits, causing confusion and misleading IoV members. The attacker does successful speculation about a genuine credential and uses it to log in to the IoV network. It is an identity attack, where the attacker could get a message from the message-distributer, and then alternates the information for his advantage [27].

(ii) GPS spoofing attack: it is a potential impersonation attack where the data attacked is precisely that of the location of vehicles or other IoV entities. Every vehicle and RSU uses GPS to provide accurate coordinates using the universal GPS. The attacker receives the correct coordinates, fakes them, and sends the wrongly generated location to the intended receiver with a signal strength higher than that of a real GPS. Reception of wrong coordinates can lead to many problems ranging from simple erroneous data to serious accidents that threaten the lives of passengers. Preventing the threat of this type of threat is a priority for the IoV system [28].

(iii) Masquerading attack: the attacker vehicle provides the ID of another vehicle as its own for an effective pretending to be that vehicle to get unauthorized access through legal access information. It is a subclass of impersonation attacks with the difference of having just one entity copying a real ID information of any node within the network [29].

(iv) Man-in-middle attack: a vehicle attacks a target vehicle using its V2V, and V2I communication by locating itself between the sender and receiver. The attacks can be either active by changing intercepted information or passive by only reading and using data for privacy challenges. GPS spoofing attacks are considered a subclass of active man-in-middles attacks [30]. Also, the data modification attack, where the attacker intercepts and modifies, deletes, or delays a message sent/received by a vehicle, is a subclass of active man-in-middle [31]. A solution to this attack is double-factor authentication.

(v) Replay attack: the attacker continues to re-transmit valid or invalid information to the target vehicle to increase the threat to the vehicle's real-time functionality. In addition to compromising conditions at the time the original message was sent, an attacker could gain access to network services and resources through this broadcast attack [32].

(vi) Cookie theft attack: like a reply attack, the attack seeks to gain unauthorized access to network resources by saving cookies and then reusing them in the network whenever needed [33].

(vii) Message injection attack: the attacker injects false information messages into the IoV system and seeks to gain access to the vehicle through the compromised electronic control unit, or the infotainment and telematics systems. Since traditional sender-receiver nodes are not authenticated by the traditional control area network, illegitimate messages will not be recognized. It is considered a data falsification attack on data integrity [34]. A fabrication attack is considered a variant of this attack, where the attacker sends false messages to customers' members, causing complete chaos on the cluster members.

(viii) Message manipulation attack: an attacker changes the message contents leading to wrong decisions of the receiving entity paralyzing the overall system [33].

(ix) Channel interference and Jamming attacks: both attacks are targeting the availability of the IoV networks. The interference attacks are performed by a third party by sending a strong signal with the same characteristics and frequency as the original V2V or V2I links. A jamming attack is accomplished by sending a signal or noise in the same bandwidth to corrupt the useful V2X signal [30]. Both can be solved by adopting modern communication schemes such as quadrature phase shift keying (QPSK), code-division multiple access (CDMA), or orthogonal frequency-division multiplexing (OFDM).

(x) Denial-of-service (DoS): the attacker sends a redundant heavy, valid message on the IoV network that is more than it can handle to jam it to the limit to stop or limit network availability. The efficiency and availability of the IoV network can be significantly affected by this type of attack similar to those used in traditional IT systems by limiting the capacity of the network service in real time. The flooding of the network by various messages can stop the critical activity of RSUs, leading to the total collapse of the IoV networks. A more sophisticated version of DoS, known as distributed DoS (DDoS) attack, exists in which the attacker may attack a system from outside to a single targeted system to agitate its functionality and network [35].

(xi) Eavesdropping attack: it is a passive attack, where the attacker is targeting the privacy and confidentiality of data by an unauthorized lessening to data exchange [30].

(xii) Message holding attack: it involves an active attacker who neglects part of the message exchange, affecting information about the road condition or the condition of the driver.

(xiii) False information flow: authenticated users can be deceived by the flow of incorrect or corrupt information causing them to believe in a false IoV environment about traffic bottlenecks and all path information. This can lead to wrong or critical decisions about path planning that can challenge the security and efficiency of the IoV system. A falsified information attack can be performed on different wireless networks at the same time, thus manipulating the whole path from the source to the destination [27].

(xiv) Channel hindrance attack: the attacker tries to interrupt the communication channels to slow down or limit the information exchange affecting the real-time application in the IoV environment [33].

(xv) Malware attack: the injection of malicious viruses and worms harm the network functionality. Also, by sending spam messages, the network bandwidth availability is challenged or limited. The resistance against this kind of attack is difficult to build because the IoV is based on decentralized architecture [34].

(xvi) Physical Vehicle damage: these attacks can be carried out by a terrorist, thief, or attacker to stop, and destroy or violate the privacy of the vehicle [36].

(xvii) Sybil attack: the target vehicle is flooded by dummy vehicles around it by generating a jamming signal from the attacker. While the path created is naturally obvious, the attacker forces the target to take a different path. Obfuscation of false information is performed using many fake identifiers issued by a single attacker in the form of a set of real nodes. The attacker, by this process, can control the IoV network challenging the security, efficiency, and consistency of the system [37].

(xviii) Fuzzy attack: the attacker focuses on studying a vehicle's behavior for a certain period to change its pattern. He sends messages by befooling the identifiers in any order using constant data hampering the functioning of the system [33].

(xix) Guessing attacks: tttackers tempt to guess vehicle identities, passwords, credentials, and biometrics of the authentic user by intercepting messages and extracting useful information from them [33].

(xx) Session linking attack: an attacker can attack by linking any of the two random sessions of any vehicle with other entities in the network which can reveal all credentials after little calculation [34].

(xxi) Black-hole attack: the attacker receives packets of information exchanged between two or more users of real opponents, who will lose all the information, causing damage to the vehicles by preventing them from packets in real time. The packets will be forwarded to another network of malicious users in the wormhole attack [30].

(xxii) Forgery attack: the attacker acts as a user device or onboard units (OBUs) and sends commands to control the network. To prevent this kind of attack, the original OBU must be protected with strong authentication steps including trusted third-party validation, so only verified users can enter the network [38].

(xxiii) Attack on fairness: vehicles participate in data collection (crowd sensing) and reporting, which allows them to receive a reward incentive. However, fairness is a challenge to balance, as drivers have an incentive to cheat in order to get more rewards than they deserve. The fairness attack is carried out by a vehicle that creates multiple identities to report false traffic information for better benefits. The misbehavior of vehicles can lead to unfairness for customers because their acquired data do not match the cost they paid. To guarantee fairness, a trusted third party is employed to verify the fairness of vehicles [39].

(xxiv) Wormhole attack: it is also known as a tunneling attack because by faking the attacker's distance from the destination node, messages from the source node are redirected to the attacker node. This creates a deadlock and exposes all the messages to the attacker node before flowing into a network. Thus, the attacker is modifying the logical network topology to collect and manipulate network traffic data [35].

Attack mapping in vehicles and their solutions are shown in Table 1. This table provides a brief overview of the most important potential attacks on the IoV network. The first column represents the asset of the attacks which can be vehicle, RSU, wireless communication channel (WCC), information, and vehicle user (VehU). The vulnerability is disclosed in the second column with its hardware and software types. In most cases, this is due to an insecure wireless communication channel (IWCC). Threats to IoV attacks are introduced in the third column. They affect system performance including privacy, data integrity, availability, and data confidentiality in general. The main attacks in the fourth column are presented in two types; they are active and passive attacks. All of these attacks are common threats to other networks and data systems but some of them have serious consequences for the IoV network. Suggested solutions can resist these attacks which are also defensive standards for all types of networks. Finally, the security component that is vulnerable to attack is introduced. It can be authentication, availability, privacy, and confidentiality.

Table 1: Attacks on vehicles and their solutions.

Asset	Vulnerability	Threat	Attack	Solution	Violated security vehicle/requirement
Vehicular (Veh.)/ user vehicular (VehU)	Insecure wireless communication channel (IWCC)	Fake identity	Masquerading	Identity-based cryptography	Authentication (Auth.) and integrity
Veh.	Software vulnerabilities	Unauthorized manipulation (UM) of comm.	Replay	Tampered proof devices	Auth.
Veh.	Disrupt ITS apply.	Message's alterations	Message injection	One time identity-based aggregate signature	Auth.
Veh., RSU	IWCC	Signal bad reception	Channel interface.	Hardware-related side Ch.	Availability
WCC.	OBU, IWCC	Infrastructure is busy	DoS and DDoS	Auth-PKI.	Availability
Information	IWCC	Private credential reveal	Eavesdropping	Encryption	Confidentiality (conf.)
WCC.	Data flow	False vehicle/RSU	Message holding	Encryption	Conf.
Veh.	OBU	UM of RT	Message deletion	Encryption	Conf.
Veh., RSU	Weak Auth.	Data alteration	Data falsification	IDS, packet message entropy/integrity	
Veh.	OBU	UM of RT	Jamming - veh. level	Spread spectrum	Availability
Veh./VehU	Software flaw	Data privacy leakage	Malware	Updating antivirus	Availability/Auth.
Veh.	Veh. hardware flaws	Disclosure of info.	Sensor impersonation	SPECS	Auth.
Veh.	OBU sensors malfunctions	Wrong info. flooding	Bogus info.	ECDSA	Auth./integrity
Veh.	Insecure cryptographic	Illegal software updates	Remote firmware updates	Secure firmware updates	Auth.
Veh./VehU.	Weak password	Privacy leakage	Social engineering	An encrypted and strong password	Integrity/Privacy
Veh.	Veh. physical access	Damaging sensors	Phy-veh. damage	Access control	Auth.
VehU	OBU and IWCC	Revelation of users' ID	User privacy disclosure	Holistic approach for data transmission	Privacy/Auth.
Information	Broadcast over IWCC	User's credentials exposure	Eavesdropping	Strongly encrypted message	Privacy/Auth.
Information	OBU and IWCC	Prevents vehicles to receive sensitive and info.	Jamming	Assign IPs to veh. and change packet delivery ratio	Availability
Information	IWCC	Message's alterations	Impersonation	Identity-based batch verification	Auth.
Information	IWCC	Message modification	MITM	Cryptographic	Availability/conf.
Information	IWCC	Message manipulation and dropping	Spoofing	Multi-antenna with secure in-region verification	Auth.
RSU and WCC central entity	Flaws in RT and nonencryption	Data leakage	Sybil	Position verification, VANET-PKI, and RobSAD	Auth./availability
WCC	IWCC	Data revelation	Eavesdropping	Encryption algorithms	Conf./privacy
RSU and the central entity	Hardware vulnerabilities	Network flooding with compromised messages	Bogus info.	ECDSA	Conf./Auth.
WCC	Hardware/software malfunction	Message alterations in route to other vehicles	MITM,RSU-central	Cryptographic techniques	Conf./availability
WCC	IWCC	Discarding messages	Wormhole	Packet leash, HEAP	Conf./Auth.

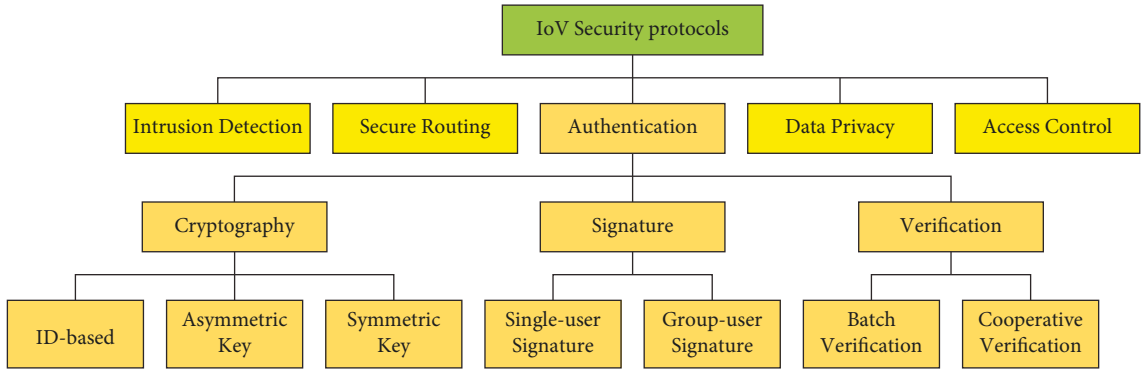

Figure 2: IoV security protocols.

3. IoV Security and Privacy

IoV as an emerging intelligent transportation system constitutes an important one as it deals with human life. Therefore, system security is the primary challenge today. Since the security layer interacts with all layers of the system, the need for robust, reliable, and applicable security technologies is an important step towards large-scale IoV deployment.

3.1. Security Protocols for IoV. The goal of the security measures is to provide a safe and secure environment for the communication of vehicles with each other and the Internet of the vehicle's management center. Security protocols in the IoV environment are classified into five classes, such as authentication, routing security, access control, data privacy, and intrusion detection as in Figure 2.

Authentication is the basic security protocol in the IoV, allowing a vehicle to authenticate itself with other vehicles and RSUs. As the vehicle is requesting to be authenticated, RSU receives a message and checks the vehicle information in the revocation list for validation. The procedure of authentication takes place through different phases and terminates with approval or denial by a trusted third party called the trusted authorities (TAs) [40]. Vehicle information is stored in the TA's database, as each vehicle has to register itself with the TA to use the network. Authentication can be performed through cryptography, signature, and verification algorithms [41]. Cryptography algorithms are using symmetric and asymmetric algorithms working on a key basis or identity-based algorithms. Keys are confidential between two communication parties because they contain some specific security instructions [42]. In the symmetric management keys, the TA is responsible for the registration of vehicles with relevant roadside units. Before doing the registration, TA calls secret keys from its memory to configure both the vehicle and roadside unit. After getting the communication path, both entities compare their secret keys that have been predefined to the route by the TA, followed by the verification of the secret key by communicating their attributes and entities [43]. In asymmetric management (public key), the authentication procedure starts with the same steps. During the registration process, they are allotted both a public and a private key, playing an important role in the security protection of the vehicle's network [44].

The private key is a secret known only to the owner and is used to encrypt messages, while the receiving node uses the corresponding public key to decrypt and authenticate the sender node. Through this encryption and decryption, we can avoid cyber-attacks easily and prevent the network from wrong guidance. After validating the request and the competencies of the roadside unit, the TA allows a vehicle to join the network through many phases which are system setup, registration, login, and dynamic node addition after the authentication process [45]. IoV security challenges require complicated security techniques to avoid hijacking and other incidents by adding measures like route modification as part of the RP security [46]. Access control is one of the oldest methods for security purposes, which plays a vital role in controlling cybersecurity attacks in the IoV environment. In the configuration of a new vehicle, the services of access control are much considered as a mechanism aiming to reduce unauthorized access in the IoV. Some of the access controls are based on static methods such as role-based access control (RBAC) and attribute-based access control (ABAC). Therefore, after the node allows access, the authorization continues. Other more advanced access controls adopt dynamic schemes [47]. If an attacker tries to violate the privacy policy of the network or data through RSU, the privacy preservation protocols act in the prevention of the system from being attackers. According to the analyst, vehicle pseudonyms will last long if they communicate through trusted authorities, and it will get a shorter life cycle if the vehicle pseudonyms communicate through nontrusted authorities [48]. Two types of intrusion detection systems exist which are local and global intrusion detection. Some research promotes intrusion prevention rather than a detection strategy for better security protection, while for motivated attackers, real-time intrusion detection is highly appreciated [35].

3.2. Attacks on In-Vehicle Systems. Vehicles are the active players in the IoV system; therefore, this section focus on the attacks targeting the in-vehicle system, as follows:

(i) Vehicle immobilizer attack: the electronic vehicle immobilizer system, also known as the physical security code (transceiver), is a standard antitheft mechanism that provides electronic security to

Table 2: Attacks on in-vehicle systems and countermeasures.

Countermeasure	Solution implementation	Prevention from	Credibility vehicle/ requirement
Ensure safe leaving	Be sure to lock off the vehicle correctly by providing a visual indicator	Jamming attack	Basic
Source signal blockage	Protect the unused key	Relay attack	Middle
Distance bounding	Rapid message transfer is employed in a distance-bounding procedure for interparty distance confirmation	Relay attack	Good
Improved authentication	Reliable and approved cryptographic algorithm and key-management system	Attacks on V-immobilizers and KESA, side-channel attacks	Good
Hidden voice detection	Interface enhancement signal analysis, audio turbulence, and liveness identification	Attacks on VCS and hidden voice commands	Good

prevent the vehicle's engine from starting up. Several commonly used transponders in the automotive immobilizer industry have been discovered as insecure in recent years [49, 50]. Hitag2 and Megamos are also broken due to the failure in the cipher architectures, such as the absence of pseudo-random number generators (PRGs) and the cipher's internal state weakness compared to traditional private keys [51]. Attacks on Hitag2 cryptographic are three, including that which reads the identity of the transponder and recovers the key-stream, a more general one that cracks generic cipher designs using linear feedback shift registers (LFSRs), and finally, an attack exploiting the crucial discovery by multiplying authentication procedures. Guerrero et al. in [6] proposed the use of AES-Rijndael encryption for car-immobilizer security.

(ii) Keyless entry-system attack (KESA): while the vehicle immobilizer system is more concerned with starting the engine, KESAs are focusing on inside-vehicle attacks. The security of data inside the vehicle is ensured by the entry mechanism. It is all thanks to technical advancements, conventional physical keys, remote active keyless, and remote passive keyless exist today [36]. Threats on KESA include jamming, replay, relay, and cryptographic analysis attacks [51].

(iii) Attacks on voice controllable systems (VCSs): VCS is an important protocol for vehicle access and control requiring strong protection. VCS is composed of three substages, which are voice capture, speech analysis and recognition, and control actions derived by voice order. In modern technology, all stages after voice capturing include digital processes through digital signal processing. Attacks on this system are hidden voice commands, Dolphin, Lipread, and audio adversarial attacks. Defending against the above threats can be carried out through various actions, including cryptography, improved authentication, scheme alteration, and other complex countermeasures including those presented in Table 2. Defending against the above threats can be done through various actions, including cryptography, improved authentication, scheme alteration, and other complex countermeasures including those presented in Table 2.

3.3. Security and Privacy Issues on IoV. IoV faces many challenges such as security, privacy, communication technology, exact location definition, and various quality of service requirements. Security and privacy preservations are the primary and challenging problems in IoV, especially in information management, storing, and using [52]. Challenges to IoV deployment can be classified into technical, social, policy, and nontechnical types [21]. Security and privacy issues fail into technical challenges focusing on the protection of data within the system. IoV is a heterogeneous network made up of several technologies, combined to form a complex system, making it more sensitive to security attacks.

Several attacks on IoV are possible, causing damage not only to drivers but also to the credibility of the entire system. The model's sensibility imposes researchers to consider all security issues such as integrity, privacy, secrecy, availability, and authentication. Due to the IoV complexity, and the variety of challenges, some researchers have suggested that this technology will need tens, if not hundreds of years to be completely protected [21]. Security and privacy vulnerabilities were among the most important issues to be addressed using IoV. Connected car technology still faces serious security and privacy issues despite serious and frequent research. Data are transferred between various entities for various system operations including value-added services and security applications. The privacy, availability, reliability, and integrity of both the user and the location data must be safeguarded et al. times [53]. A considerable amount of effort has previously been expended to decrease different forms of vehicle data-related risks in IoV [9].

3.3.1. Privacy. Security is interested in the secrecy of important data, while privacy is concerned with who or what they are protecting the data from. Privacy in IoV is very close, but it is not equal to data confidentiality, which has a lower-volume concept of keeping data as confidential as possible. Privacy is a leading role in the IoV network, in

Table 3: Privacy and security issues.

Attacks	[39]	[55]	[56]	[5]	[57]	[58]	[59]	[60]	[61]	[62]	[63]	[64]
Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X
Forgery	✓	X	✓	X	X	X	X	X	X	✓	X	X
Trusted third-party validation X	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓
Impersonation	✓	X	✓	✓	X	X	✓	X	X	X	X	X
Sybil	✓	X	X	X	X	X	X	✓	X	X	X	X
Privacy techniques for vehicles	✓	✓	✓	✓	✓	✓	X	X	✓	X	✓	X
Fairness	✓	✓	✓	X	X	✓	X	X	X	X	X	X
Man in the middle	X	X	✓	X	X	X	X	X	X	X	X	X
DDoS	X	X	X	X	X	X	✓	X	X	X	X	X
DoS	X	X	✓	✓	X	X	X	X	X	✓	X	X
Replay	X	X	✓	✓	X	X	X	X	X	✓	X	X
Data nonrepudiation	✓	✓	✓	✓	✓	✓	X	X	X	X	X	X
Access control	✓	✓	✓	X	✓	X	X	X	X	X	X	X
Session key security	X	X	✓	X	X	X	X	X	X	✓	X	✓
Eavesdropping	X	X	X	X	X	X	X	X	X	✓	X	X
Data encryption	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy techniques for navigation	✓	✓	✓	✓	✓	✓	X	X	X	X	✓	X
Collusion resistance	X	X	✓	X	✓	✓	X	X	X	X	X	X
Data integrity	X	✓	✓	✓	✓	✓	X	✓	✓	X	X	X
Auxiliary	X	X	X	X	X	X	✓	X	X	X	X	X

which there is no trust in any service if privacy is violated. Therefore, privacy is a pivotal point in protecting IoV from many threats [54]. As part of IoV technology, vehicles share collected information about locations, traffic conditions, speed, and environmental information with other vehicles. This can help predict a driver's social behavior by retracing their trajectory, activity, and sensory information that exposes the potential for privacy violations. Several methods are used to prevent privacy attackers from accessing reasonable data, such as the use of anonymization techniques through information sharing, with identity hiding [39]. Table 3 outlines many defenses, and security-privacy concerns and depicts a connection that expresses all the issues posed in the various articles. This helps to identify serious problems and reduce corresponding appropriate solutions.

3.3.2. Integrity. Integrity is the quality describing the reliability, coherence, and validity of data exchanged between various entities or stored in the system. The permanent correctness of data is challenged by many attacks such as message tampering, masquerading, black hole, gray-hole, fabrication, and malware. Integrity protects data from being tampered with or changed by an unauthorized party. Internal attacks by registered attackers, such as message injection or data manipulation, will generally compromise integrity [65]. Attacks on vehicular networks can lead to traffic manipulation, and incorrect knowledge can lead to traffic collisions. The most frequent attack that compromises integrity service is the active man-in-the-middle attack. Authentication and data encryption are active measures to protect IoV against integrity attackers. Group key-management scheme includes group handover for group-based authentication and key agreement. This scheme is an active remedy for men-in-the-middle (active and passive), eavesdropping, impersonation, and denial-of-service (DoS) attacks [66]. Table 4 outlines many integrity attacks.

Table 4: Attack on integrity.

Attacks	[67]	[68]	[69]	[70]	[71]	[72]	[73]
DoS attack	✓	X	X	X	X	X	X
Jamming attack	✓	X	✓	X	X	X	X
Message tampering attack	✓	✓	X	X	X	X	X
Bogus status update attack	✓	X	X	X	X	X	X
Masquerade attack	X	✓	✓	✓	✓	X	X
Black-hole attack	X	X	✓	X	✓	X	✓
Malware attack	X	X	X	X	✓	X	X
Gray hole attack	X	X	✓	X	X	✓	✓
Fabric- ation attack	X	X	X	X	✓	✓	✓

3.3.3. Availability. IoV system availability describes the reliable access of the network as data, resources, and services at any time. It is connected to the scalability of the system when the number of network users grows, so an operation breakdown is expected or at least a deterioration of offered services. As a result, one of the IoV system's primary obligations is to make itself accessible to all legal users. Using cloud computing, a whole new way of open assault has been identified against availability such as DoS, black hole, gray hole, spamming, jamming, and ransomware attacks are some of the potential attacks on availability. For vehicular networks, availability is another crucial protection feature. Autonomous cars must be able to obtain traffic and route information without interruptions, or they risk causing traffic collisions or gridlock. Any legal vehicle should be able to access and use services whenever and wherever it is required. Denying real users access to the technology will allow cloud attackers to mount a sustained DoS assault that hurts legitimate users [74]. DoS, as well as distributed denial of service (DDoS), put at risk the availability of vehicular network activity. DoS attacks will be successful if the

Table 5: Attack on availability.

Attacks	[70]	[28]	[71]	[75]
DoS attack	✓	✓	✓	X
Spamming attack	X	✓	✓	X
Jamming & malware attacks	X	✓	X	✓

attackers can use all the bandwidth to submit fraudulent primary authentication certificates. It is important to provide an effective co-authentication scheme to prevent this attack. Table 5 outlines the many Integrity attacks.

A second important threat to availability is spamming, which is by sending spam communications across the network, consuming bandwidth, and disrupting normal packet latency across the network. Antispam classification algorithms offer a good solution to this problem. Finally, jamming is a classical but active attack scenario used for a long time against communication and especially wireless channels. Modern communication modulation and coding such as CDMA, QAM, and OFDM present an active countermeasure against jamming. Table 5 outlines the most important threats to availability and a selection of research on the topic.

3.3.4. Authentication. Authentication is the act of identifying the acting party through a mechanism based on credential information that must be validated by a trusted entity, which is called TA. It is the most important security protocol used for IoV security, taking place at many levels and locations in the system. To join a cluster, a vehicle must be authenticated by the RSU by checking its credential information, and also it is required to validate the authenticity of results within the system. Vehicle sends joining request to the closet RSU with primary information, and RSU processes the request by sending it to the TA. TA checks the authenticity of the information direct-source RSU, validates the vehicle information, and sends back an accept-join or reject-join to the RSU through a secure channel.

A strong authentication procedure has a direct impact on data privacy, integrity, availability, and security in general. It is true to say that authentication is considered the first front line of defense for all networks, and especially for the IoV. The system should be eligible to distinguish between fair vehicles and crooked vehicles that are crooked by a robust authentication process to eliminate or limit at maximum Sybil, masquerading, replay, message injection, warm hole, and GPS deception attacks [37]. An assault on IoV authentication can be carried out by either intracluster or out-cluster methods. The attack can directly compromise the authentication system by allowing attackers to obtain the private credentials of valid nodes to access private information that could deceive the network's entities.

Authentication techniques can be classified into many categories according to many variables such as method, mechanisms, used algorithm, and application. The classification based on authentication mechanisms and algorithms into five types looks to be general and practical. Authentication types are lightweight, hash-based, batch verification-based, dual, and privacy-preserving authentication [33]. Since a weak authentication procedure leads to exposing entity's private data to an unauthorized person, a privacy-based authentication mechanism is of great importance. A Summary of characteristics of privacy-preserving authentication protocols is given in Table 6. Message authentication codes (MACs) or challenge-response protocols are two popular approaches to solving authentication and identity issues. Both methods offer sender verification, but they also apply additional computing overhead to the scheme, which can pose new challenges [33]. The increased computing overhead imposed by authentication mechanisms infringes on these devices' real-time restrictions or resource limits. Aside from MACs and challenge-response implementations, much of the research on IoV authentication and identification has shifted to the concept of using pseudonyms instead of vehicle identities to have better protection but requiring improved computing facilities. However, since the pseudonym requires undesired computing overhead during the security process, the authentication of the attribute-based credential has been proposed as a robust, reliable substitute [80]. Table 7 presents the most significant attacks on IoV authentication, which have been addressed by several recent research papers.

4. Blockchain

BC is a popular distributed ledger technology, aiming to provide a secure, trustworthy, scalable environment, and efficient way to satisfy various IoV needs. It has completely changed many fields such as cryptocurrency, IoT, healthcare, logistic, and many governmental applications. This technology has gained significant research interest in smart transportation including IoV systems. In the future vision of IoV, all vehicles will be connected to the Internet, and the BC will support this network and get the system out of centralization to decentralization at a low cost.

4.1. Blockchain Structure. Blockchain (BC) is defined as a process of storing data that makes it very hard or unattainable to log in, change it, or defraud it. It is a distributed-decentralized database of operations that is duplicated and replicated by the BC's whole network, first known in the security implementation of digital coins [89]. The BC is a data management technology, stores the complete list of operations in a set of blocks that are connected in the same way as a linked list. The first block of the BC is known as the "zero block" or "genesis block," and it retains transaction ownership by not relating to previous blocks. The block of a BC is logically partitioned into header and body [90]. A block's header stores information about all blocks, such as the block hash, the previous block's hash, block timestamp, block index, and Merkle root. The public key technique (private-public pair) is needed to validate data in BC transactions, such as cryptocurrency or data exchange. A BC's member nodes use their private keys to verify transactions. There are three existing types of BC, which are

Table 6: Summary of characteristics of privacy-preserving authentication protocols.

Scheme	Concept applied	Network model entities	Phases or steps	Benefits and limitations
[76]	Physical unclonable functions providing a challenge-response mechanism	RSU, RSU gateway, and TA	A vehicle needs to authenticate only once when it enters the area of an RSU gateway	Authentication, reduced authentication overhead, high throughput, and robustness against various attacks
[77]	A safety-aware location privacy-preserving scheme	RSU,TA, server-based	System initialization phase basic safety message car registration phase	Authentication and better location privacy levels while still fulfilling the road-safety requirements
[78]	Elliptic curve crypto. Diffie–Hellman–Schnarr signature, timestamps	TA, RSU, and application server	System initialization phase anonymous identity generation message signing phase message verification phase	Authentication, privacy-preserving, robust against impersonation, modification, stolen verifier, man in the middle attack, and the low computational cost
[79]	A blockchain-based secure and privacy-preserving authentication protocol	Registration authority BC-based authentication and VSN cooperative comm.	System initialization phase vehicles connect to LAC authentication verification-BC and the message verification phase	Fast authentication, improved reliability, confidentiality, nonrepudiation, integrity, and privacy

Table 7: Attack on authentication.

Attacks	[81]	[17]	[82]	[9]	[58]	[83]	[84]	[85]	[86]	[76]	[87]	[4]	[88]
Identity authentication	✓	✓	✓	X	X	✓	X	X	✓	X	X	X	✓
Identity counterfeiting	✓	X	X	X	✓	✓	✓	X	✓	✓	X	X	X
Sybil attack	X	X	✓	✓	X	X	X	X	X	X	✓	X	✓
Masquerading attack	X	X	X	✓	X	X	X	X	X	X	X	X	X
Wormhole attack	X	X	X	✓	X	X	X	X	X	X	X	X	X
Replay attack	X	X	X	✓	✓	X	X	X	✓	X	X	✓	✓
Spoofing attack	✓	X	X	X	✓	X	X	X	✓	X	X	X	X
DDoS attack	X	X	X	X	X	X	✓	X	X	✓	X	X	X
Man-in-the-middle attacks	X	✓	X	X	X	X	✓	✓	X	X	X	X	X
Impersonation attack	X	✓	X	X	X	X	✓	✓	✓	X	X	X	X
Traceability attacks	X	X	X	X	X	X	X	✓	✓	X	X	X	X
Jamming attack	X	X	X	X	X	X	X	X	✓	X	X	X	X

public, private, and hybrid BCs [2]. The public is available for anyone to join and access. Cryptocurrency networks are an example of these BCs (Bitcoin, Ethereum, and Altcoin). A private BC is an under permission-BC that only the known members of a particular entity can use. It is partly immutable and does not require any currency or payment fee or processing fee for transactions. IoV security can be improved by the use of such BC type. Hybrid BC known also as consortium BC is a private-public type. BC technology is a promising tool for IoV security because of its characteristics which are [91] as follows:

(i) Decentralization: the BC is built on a modular model that eliminates the need for a central authority which may be used to have flexible protection solutions.

(ii) Availability: there is no single point of failure since the BC is decentralized. As a result, the system's security and availability have been strengthened.

(iii) Cryptocurrency exchanges: several BC ledgers provide cryptocurrency trading services. It may be a cost-effective way to build reliable, safe, and automated reward systems that enhance the vehicle's cooperation.

(iv) Transparency: the substance of the BC ledger is accessible to all nodes in a BC network.

(v) Immutability: the BC ledger's data cannot be changed. As a result, the BC offers an easy and effective method of storing protected data.

(vi) Pseudonymity: BC assigns a pseudonymous address to each person. This may be a way to make privacy-preserving programs more widely available.

(vii) Automatic car trades: using a smart contract, vehicle exchanges can be automated. As a result, data exchange resource-sharing services may be implemented without the need for human interaction.

4.2. BC-Based Application for IoV. Decentralization, affordability, immutability, confidentiality, and exchange automation are all advantages of BC technology. As a result,

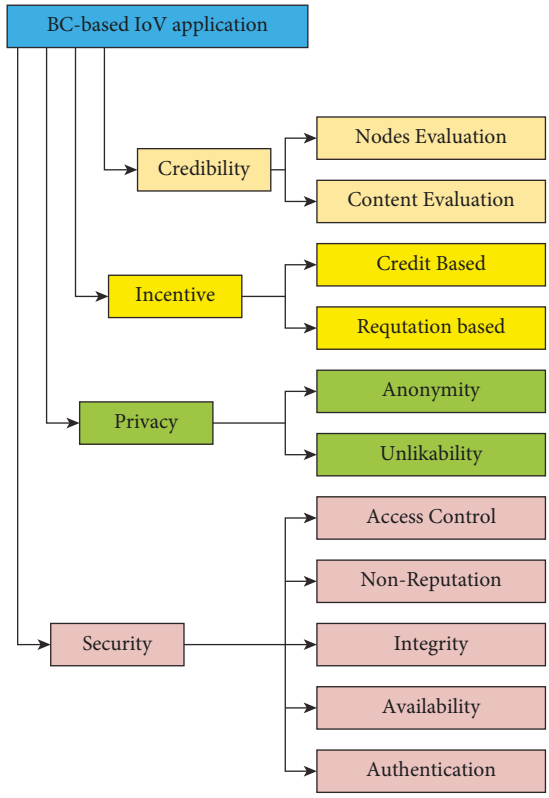

Figure 3: BC-based IoV.

BC could be a cost-effective method to develop the IoV system into one that is trustworthy, stable, and private. Four important applications have already been developed for BC-based IoV: security (transparency and immutability), credibility (automation exchange, transparency, and others), incentive credit-based incentive, and preservation of privacy as shown in Figure 3 [91].

While security, credibility, and privacy application are well defined, the credit-based incentive is an encouragement for IoV entities to share their computing, storage, and networking capabilities by receiving credits for their contribution. IoV links a vast number of vehicles for information sharing such as collisions, incident updates, traffic, weather, and infotainment messages, among others. When contemplating the timely distribution of information while still ensuring network scalability, implementing a consolidated vehicular infrastructure for handling such a large volume of data is exceedingly difficult [92]. Since sensitive data are shared between intelligent vehicles, V2X communications are vulnerable.

The security requirements of intelligent IoV systems are data provenance, transparency, resilience, and immutability. Without the intervention of a central authority, BC meets these requirements by establishing confidence between different vehicles in a challenging environment. Decentralization is one of the key features of blockchain, which preserves and stores event information clearly and permanently while also transmitting it in a timely, stable, and distributed manner [93]. The BC's underlying capabilities aid in achieving metadata traceability and accountability in the IoV network, which can be trusted data presenting pieces of evidence during accidents and other problems [94]. As a result, BC offers several benefits, including shielding the stability and anonymity of vehicular nodes from various forms of sophisticated cyber-attacks. This ensures knowledge immutability and stability in the face of unexplained vehicular network attacks. As many vehicular nodes access blockchain networks, the system's durability is ensured. The initial blockchain will also be open to all member vehicular nodes even though those vehicles went offline or were inaccessible due to malicious code, car malfunctions, or cyber-attacks. In blockchains, all events or transactions are timestamped and authenticated using private keys. Vehicle owners may monitor the history of purchases and events or incidents at any given moment in a safe manner. Table 8 presents important research on BC-based solutions to the attacks on security and privacy in IoV and other unmanned vehicle systems. While all the attacks and the protection measures mentioned in this table are explained throughout this research, k-anonymity is used to protect the privacy of vehicles. Attackers are unable to separate vehicles based on swarm detection information. In a group of k similar vehicles, k-anonymity is a classical privacy-preserving, in which the target is indistinguishable from the other $k-1$ group members [98]. The probability of target identification is $1/k$, so the rank of anonymity depends on k and the foreknowledge of the attacker.

5. Current Surveys and Reviews

The diversity of threats to an IoV comes from a variety of types of interelement communication, the number of sensor elements involved, the system architecture, mobility, and the real-time operational characteristic of the network. This includes threats to privacy, confidentiality, integrity, and availability. To protect the system from these threats, significant overheads are added to the cost of computing and communications, and this reflects negatively on network availability. The latest IoV security review and survey papers show an increasing interest in the topics with the number and quality of publications. After careful examination of a large number of review and survey papers, a sample of publications was selected due to their comprehensive and detailed coverage of the topic, as well as its recentness. A comparison is given in Table 9 between these works and our review paper outlining the most important aspects of a good review paper such as publication year (Year), IoV architecture (Arch.), attack analysis (A-analysis), privacy, integrity, availability, length of paper (S-short, M-medium, and L-long), and suggestion of new solutions (n-solution). Since BC-based IoV security is an important and promising technology, a number of research studies in this area are included in the comparison.

A newly published survey examining the use of blockchain and federated learning (FL) as emerging technologies to solve security problems in IoV is presented in [112]. FL by its Distributed Learning (DL) capability and Artificial Intelligence (AI) based computation can be a good solution for provision of privacy protection in IoV. Moreover, DL and AI

Table 8: BC-based IoV.

Attacks	[95]	[81]	[96]	[97]	[98]	[99]	[100]	[101]	[102]	[103]	[104]	[105]	[106]	[107]	[108]	[109]	[110]	[111]
Identity validity	✓	✓	X	X	X	X	✓	X	X	X	✓	X	✓	✓	X	X	X	✓
Authentication	✓	✓	X	✓	✓	X	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy	X	X	✓	X	✓	✓	X	✓	✓	X	X	X	✓	X	X	X	X	X
Malicious attacks	X	✓	✓	X	X	✓	X	X	X	✓	X	X	X	✓	X	✓	✓	X
Dos attack	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Firmware integrity	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
K-anonymity protection	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X
Integrity	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X
Illegal data tampering	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X
Sybil	X	X	X	X	X	X	X	X	✓	✓	X	X	X	X	✓	X	X	X
Replay attacks	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X
Impersonation	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X
Public key tampering	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X
Tracking	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X
Black-hole	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X
Spoofing	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓

Table 9: Comparative study on existing surveys in IoV security.

Ref.	[27]	[83]	[2]	[17]	[33]	[80]	[112]	(Our review)
Year	2019	2019	2020	2020	2020	2021	2022	2022
Arch.	✓	✓	X	X	✓	X	✓	✓
Attacks analysis	✓	X	✓	X	✓	X	X	✓
Privacy	✓	✓	✓	✓	✓	✓	✓	✓
Integrity	✓	X	✓	X	✓	✓	✓	✓
Availability	✓	X	✓	X	✓	✓	✓	✓
Paper length	L	L	M	M	L	S	M	M
New solution	X	✓	✓	✓	✓	✓	✓	✓

capabilities can resolve communication overhead issues that arose from collecting data from multiple nodes and storing it in a central location. FL uses machine learning (ML) and deep learning (DL) algorithms to train data within its scope. FL addresses the problem of centralized data through a distributed ML/DL approach and is trained globally, and then the updated parameters are distributed across the server to the end-machines, where the FL process can start to ensure the privacy of IoV elements. Referring to the analysis and comparison, our review demonstrates a better overall understanding of the challenges and trends in IoV security by including all the threats, solutions, and trends suggested in the newly published works.

6. Challenges and Future Directions

IoV security is a very active area of research where every introduced work has its new solutions to overcome system security challenges. New technology can also provide some solutions to system limitations such as computing and power resources improvement, allowing the use of classical standards or innovative methods to solve security problems. After going through the literature, some open issues and future research directions are identified:

(i) New solutions for existing threats: data privacy, confidentiality, and availability remain among the most important challenges facing the modern transportation system. The heterogeneity of the IoV system, as well as the large and diverse number of parties involved, make this problem difficult to solve. Federal education (FL) combined with blockchain brings emerging technologies to solve this problem. FL can be a good solution to protect IoV privacy system availability by reducing communication overhead. Data confidentiality can be achieved through the use of blockchain [112].

(ii) System architecture complexity: most IoV security proposals do not take into account the complexity of the system communication architecture such as switching a vehicle between two RSUs or communicating between two vehicles connected to different RSUs. Strong security measures in RSU-2-RSU communications and clustering-based vehicle topology using a distributed database can provide a solution to this problem.

(iii) Development of lightweight encryption: data security in IoV is still handled using classical (symmetric and asymmetric) encryption standards. The availability, mobility, computing power, and real-time nature of an IoV system require the use of a fast, lightweight, and secure data encryption

standard. Specific standards for lightweight data encryption for a dynamic IoV environment have not yet been formally developed or approved. Most of the proposed solutions are based on available lightweight algorithms, classic standards such as AES, or hybrid encryption based on both families.

(iv) Processing unit: IoV is a dynamic network that undergoes topological change, and its high mobility has led to a large number of new communication activities between vehicles and RSUs. Also, the exchange of data between vehicles within a single driving region as part of social IoV (SIoV) makes in-vehicle computing a significant and critical point. The system may require high-speed processing units and an innovative algorithm for data compression, encoding, and communication [30].

(v) Localization system: the localization system used in IoV is mainly based on the use of the global positioning system (GPS). Navigation, correct location collection, and safe transmission of vehicle location to avoid accidents are of paramount importance. GPS is known for its precise data which can be used as key location information with appropriate security measures. Integrating GPS data with other sensor data (location and distance sensors) to avoid accidents between vehicles presents new research objectives. All these navigation systems can serve as a unified vehicle proximity tracking system that prevents accidents with other vehicles.

(vi) Secure big data analytics: big data is generated by SIoV that requires the collection, transmission, storage, classification, and decision making. Data mining, classification using artificial intelligence tools, and blockchain-based distributed databases provide a broad research direction.

7. Conclusion

In this review article, the need for permanent monitoring of the security and privacy challenge-solution in IoV is addressed. The importance of intelligent transportation security, especially in IoV, is analyzed from different perspectives due to its critical nature related to human life and quality of life. The privacy concerns of the system are also presented because IoV must be regarded as a privacy-preserving system having direct contact with people's data. Attacks are classified according to their targets, nature (physical or cyber), issued location (internal or external), and where proposed solutions are presented. They are linked to security targeted protocol so the solution can easily be summarized. The security protocols are explained and the most important body of knowledge on the subject is presented in a comprehensive manner using tables. Blockchain, as a promising technology improvement, has been presented with important steps of research related to IoV security. Our future endeavors will be focused on addressing the security concerns as identified in this review paper.

Data Availability

No underlying data on an external basis were used to support the results of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[2] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: a systematic review," *Computers & Electrical Engineering*, vol. 86, Article ID 106717, 2020.

[3] B. Ji, X. Zhang, S. Mumtaz et al., "Survey on the internet of vehicles: network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34–41, 2020.

[4] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transport and Telecommunication Journal*, vol. 19, no. 4, pp. 325–334, 2018.

[5] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[6] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," *IEEE Wireless Communications*, vol. 22, no. 6, pp. 122–128, 2015.

[7] L. S. Abdulla, M. K. Mahmood, A. F. Salih, and S. M. Karim, "Analysis and evaluation of symmetric key ciphers for internet of things smart home," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 1191–1198, 2021.

[8] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry, and D. Giri, "A robust elgamal-based password-authentication protocol using smart card for client-server communication," *International Journal of Communication Systems*, vol. 30, no. 11, p. e3242, 2017.

[9] N. Sharma, N. Chauhan, and N. Chand, "Security challenges in internet of vehicles (iov) environment," in *Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication*, pp. 203–207, IEEE, Jalandhar India, December 2018.

[10] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks*, vol. 2021, Article ID 5554318, 9 pages, 2021.

[11] S. A. Chaudhry, "Combating identity de-synchronization: an improved lightweight symmetric key based authentication scheme for iov," *Journal of Network Intelligence*, vol. 6, no. 12, 2021.

[12] N. Liu, "Internet of vehicles: your next connection," *Huawei WinWin*, vol. 11, pp. 23–28, 2011.

[13] F. Bonomi and C. Fellow, "The smart and connected vehicle and the internet of things," *Invited Talk, Workshop on Synchronization in Telecommunication Systems*, 2013.

[14] F. D. Da Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. A. Loureiro, *Data communication in vanets: a survey,*

challenges and applications, Ph.D. dissertation, INRIA Saclay; INRIA, Rocquencourt, France, 2014.

[15] A. H. Sodhro, G. H. Sodhro, M. Guizani, S. Pirbhulal, and A. Boukerche, "Ai-enabled reliable channel modeling architecture for fog computing vehicular networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 14–21, 2020.

[16] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 2014.

[17] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "Iov-smap: secure and efficient message authentication protocol for iov in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.

[18] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled internet of vehicles with cooperative positioning: a deep neural network approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3485–3498, 2020.

[19] Y. Cao, C. Xiao, B. Cyr et al., "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2267–2281, London U K, November 2019.

[20] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 829–846, 2018.

[21] R. Hussain and S. Zeadally, "Autonomous cars: research results, issues, and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1275–1313, 2019.

[22] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, 2019.

[23] W. Xu, H. Zhou, N. Cheng et al., "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[24] O. Kaiwartya, A. H. Abdullah, Y. Cao et al., "Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[25] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero Ibáñez, "A seven-layered model architecture for internet of vehicles," *Journal of Information and Telecommunication*, vol. 1, no. 1, pp. 4–22, 2017.

[26] L. Alouache, N. Nguyen, M. Aliouat, and R. Chelouah, "Survey on iov routing protocols: security and network architecture," *International Journal of Communication Systems*, vol. 32, no. 2, pp. 1–19, 2019.

[27] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in vanets: communication, applications and challenges," *Vehicular Communications*, vol. 19, pp. 1–36, 2019.

[28] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[29] M. Azees and P. Vijayakumar, "Cekd: computationally efficient key distribution scheme for vehicular ad-hoc networks," *Australian Journal of Basic and Applied Sciences*, vol. 10, no. 2, pp. 171–175, 2016.

[30] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Security and Privacy*, vol. 1, no. 5, p. e39, 2018.

[31] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in vanet security: a survey," in *Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference*, pp. 1–7, IEEE, Boston, MA, USA, September 2015.

[32] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, Article ID 100214, 2020.

[33] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54 314–354 344, 2020.

[34] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[35] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: vanets and iov," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[36] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the 18th Network and Distributed System Security Symp*, The Internet Soc, Zurich, Switzerland, 2011.

[37] J. Li, Z. Xue, C. Li, and M. Liu, "Rted-sd: RTED-SD: a real-time edge detection scheme for sybil DDoS in the internet of vehicles," *IEEE Access*, vol. 9, pp. 11296–11305, 2021.

[38] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in iov," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, p. 5409, 2020.

[39] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146–152, 2017.

[40] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban vanet networks," *Journal of Information Security and Applications*, vol. 58, Article ID 102779, 2021.

[41] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[42] M. A. Saleem, K. Mahmood, and S. Kumari, "Comments on "akm-iov: authenticated key management protocol in fog computing-based internet of vehicles deployment"," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4671–4675, 2020.

[43] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[44] S. V. Mahagaonkar and N. Dongre, "Teac: timed efficient asymmetric cryptography for enhancing security in vanet," in *ProceeInternational Conference on Nascent Technologies in Engineering*, pp. 1–5, IEEE, Vashi, India, January 2017.

[45] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, "Three-factor authentication protocol using physical unclonable function for iov," *Computer Communications*, vol. 173, pp. 45–55, 2021.

[46] M. A. Ferrag and A. Ahmim, "Esspr: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommunication Systems*, vol. 66, no. 3, pp. 481–503, 2017.

[47] Y. Liu, M. Xiao, Y. Zhou et al., "An access control mechanism based on risk prediction for the iov," in *Proceedings of the 2020 IEEE 91st Vehicular Technology Conference*, pp. 1–5, IEEE, Antwerp, Belgium, May 2020.

[48] J. Li, H. Lu, and M. Guizani, "Acpn: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[49] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled rfid device," *USENIX Security Symposium*, vol. 31, pp. 1–16, 2005.

[50] R. Verdult, F. D. Garcia, and B. Ege, "Dismantling megamos crypto: wirelessly lockpicking a vehicle immobilizer," in *Supplement to the Proceedings of 22nd {USENIX} Security Symposium*, pp. 703–718, 2015.

[51] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: threats, defenses, and future directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, 2020.

[52] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in iov," *IEEE Systems Journal*, vol. 15, no. 1, pp. 245–256, 2021.

[53] F. Ahmad, A. Adnane, and V. N. Franqueira, *A Systematic Approach for Cyber Security in Vehicular Networks*, pp. 38–62, Scientific Research Publishing, Derby, UK, 2016.

[54] Y. Bevish Jinila, G. Merlin Sheeba, and S. Prayla Shyry, "Ppsa: privacy preserved and secured architecture for internet of vehicles," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3271–3288, 2021.

[55] J. Ni, X. Lin, K. Zhang, and Y. Yu, "Secure and deduplicated spatial crowdsourcing: a fog-based approach," in *Proceedings of the IEEE Global Communications Conference*, pp. 1–6, IEEE, Washington DC USA, December 2016.

[56] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *Journal of Network and Computer Applications*, vol. 134, pp. 89–99, 2019.

[57] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2018.

[58] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[59] J. Joy and M. Gerla, "Internet of vehicles and autonomous connected car-privacy and security issues," in *Proceedings of the 2017 26th International Conference on Computer Communication and Networks*, pp. 1–9, IEEE, Vancouver, BC, Canada, July 2017.

[60] L. Zhu, C. Zhang, C. Xu et al., "Prif: a privacy-preserving interest-based forwarding scheme for social internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2457–2466, 2018.

[61] M. A. Habib, M. Ahmad, S. Jabbar et al., "Security and privacy based access control model for internet of connected vehicles," *Future Generation Computer Systems*, vol. 97, pp. 687–696, 2019.

[62] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644–655, 2019.

[63] L. Wang and X. Liu, "Notsa: novel obu with three-level security architecture for internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3548–3558, 2018.

[64] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: architecture, use case, and security and forensic challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, 2017.

[65] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5g mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[66] E. T. Sağlam and Ş. Bahtiyar, "A survey: security and privacy in 5g vehicular networks," in *Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK)*, pp. 108–112, IEEE, Samsun, Turkey, September 2019.

[67] M. M. Hossain, R. Hasan, and S. Zawoad, "Trust-iov: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (Iov)," in *Proceedings of the 2017 IEEE International Congress on Internet of Things*, pp. 25–32, ICIOT, Honolulu, HI, USA, June 2017.

[68] M. Amoozadeh, A. Raghuramu, C.-N. Chuah et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[69] A. M. Abdelgader, F. Shu, W. Zhu, and K. Ayoub, "Security challenges and trends in vehicular communications," in *Proceedings of the 2017 IEEE Conference on Systems, Process and Control (ICSPC)*, pp. 105–110, IEEE, Meleka, Malaysia, December 2017.

[70] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[71] A. S. Al Hasan, M. S. Hossain, and M. Atiquzzaman, "Security threats in vehicular ad hoc networks," in *Proceedings of the 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 404–411, IEEE, Jaipur, India, September 2016.

[72] P. Wang, G. Yu, X. Wu, H. Qin, and Y. Wang, "An extended car-following model to describe connected traffic dynamics under cyberattacks," *Physica A: Statistical Mechanics and Its Applications*, vol. 496, pp. 351–370, 2018.

[73] R. Mishra, A. Singh, and R. Kumar, "Vanet security: issues, challenges and solutions," in *Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 1050–1055, IEEE, Chennai, India, March 2016.

[74] A. Samad, S. Alam, S. Mohammed, and M. Bhukhari, "Internet of vehicles (iov) requirements, attacks and countermeasures," in *Proceedings of the 12th INDIACom*, pp. 4037–4040, New Delhi, India, March 2018.

[75] V. L. Thing and J. Wu, "Autonomous vehicle security: a taxonomy of attacks and defences," in *Proceedings of the IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, pp. 164–170, IEEE, Chengdu, China, December 2016.

[76] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.

[77] M. Babaghayou, N. Labraoui, A. A. Abba Ari, M. A. Ferrag, L. Maglaras, and H. Janicke, "Whisper: a location privacy-preserving scheme using transmission range changing for internet of vehicles," *Sensors*, vol. 21, no. 7, p. 2443, 2021.

[78] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[79] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, A. S. M. Kayes, and A. Zengin, "A blockchain-based authentication protocol for cooperative vehicular ad hoc network," *Sensors*, vol. 21, no. 4, p. 1273, 2021.

[80] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: classification and challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, 2021.

[81] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, no. 072, pp. 45061–45072, 2019.

[82] D. S. Reddy, V. Bapuji, A. Govardhan, and S. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," in *Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies*, pp. 1–5, IEEE, Chennai, February 2017.

[83] X. Wang, Z. Ning, M. Zhou et al., "Privacy-preserving content dissemination for vehicular social networks: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2019.

[84] M. S. Eddine, M. A. Ferrag, O. Friha, and L. Maglaras, "Easbf: an efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles," *Journal of Information Security and Applications*, vol. 59, Article ID 102802, 2021.

[85] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5535–5548, 2020.

[86] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, pp. 29–39, 2021.

[87] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6g: machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2020.

[88] S. Sharma, K. K. Ghanshala, and S. Mohan, "Blockchain-based Internet of Vehicles (Iov): An Efficient Secure Ad Hoc Vehicular Networking Architecture," in *Proceedings of the 2019 IEEE 2nd 5G World Forum*, pp. 452–457, IEEE, Dresden, Germany, September 2019.

[89] T. Alharbi, "Deployment of blockchain technology in software defined networks: a survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[90] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[91] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in internet of vehicles," *Computers & Electrical Engineering*, vol. 84, Article ID 106646, 2020.

[92] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand computing resource trading in iov-assisted smart city," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1373–1385, 2021.

[93] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[94] P. Helo and Y. Hao, "Blockchains in operations and supply chains: a model and reference implementation," *Computers & Industrial Engineering*, vol. 136, pp. 242–251, 2019.

[95] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58 241–258 254, 2019.

[96] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[97] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proceedings of the 2019 IEEE Wireless Communications and Networking Conference*, pp. 1–7, IEEE, Marrakesh, Morocco, April 2019.

[98] M. D. Firoozjaei, A. Ghorbani, H. Kim, and J. Song, "Evchain: a blockchain-based credit sharing in electric vehicles charging," in *Proceedings of the 2019 17th International Conference on Privacy, Security and Trust*, pp. 1–5, IEEE, Fredericton, NB, Canada, August 2019.

[99] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[100] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, G. Linchao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion*, pp. 139–145, IEEE, Lisbon, Portugal, July 2018.

[101] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 2019.

[102] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in vanet," *Sensors*, vol. 19, no. 22, p. 4954, 2019.

[103] A. Mostafa, "Vanet blockchain: a general framework for detecting malicious vehicles," *Journal of Communications*, vol. 14, no. 5, pp. 356–362, 2019.

[104] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "Bbaas: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in Vanets," *Security And Communication Networks*, vol. 2021, 11 pages, 2021.

[105] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for vanet with blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5836–5849, 2020.

[106] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in vanets," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[107] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in vanet," *Vehicular Communications*, vol. 30, Article ID 100350, 2021.

[108] A. Haddaji, S. Ayed, and L. C. Fourati, "Blockchain-based multi-levels trust mechanism against sybil attacks for vehicular networks," in *Proceedings of the 2020 IEEE 14th International Conference on Big Data Science and Engineering*, pp. 155–163, IEEE, Guangzhou, China, December 2020.

[109] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in vanet routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, 2021.

[110] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in vanet," in *Proceedings of the 2018 IEEE 3rd International Conference on Computing, Communication and Security*, pp. 161–166, IEEE, Kathmandu, Nepal, October 2018.

[111] C. Dai, X. Xiao, Y. Ding, L. Xiao, Y. Tang, and S. Zhou, "Learning based security for vanet with blockchain," in *Proceedings of the 2018 IEEE International Conference on Communication Systems*, pp. 210–215, IEEE, Chengdu, China, December 2018.

[112] A. R. Javed, M. A. Hassan, F. Shahzad et al., "Integration of blockchain technology and federated learning in vehicular (iot) networks: a comprehensive survey," *Sensors*, vol. 22, no. 12, p. 4394, 2022.