Received: 31 December 2020 | Revised: 1 April 2021 | Accepted: 25 April 2021

DOI: 10.1002/ett.4317

SPECIAL ISSUE ARTICLE

WILEY

A survey on the blockchain techniques for the Internet of Vehicles security

Sathish Kumar[1] | **Sarveshwaran Velliangiri**[2] | **Periyasami Karthikeyan**[3] | **Saru Kumari**[4] | **Sachin Kumar**[5] | **Muhammad Khurram Khan**[6]

[1]Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, Ohio,

[2]Department of Computer Science and Engineering, B V Raju Institute of Technology, Medak, India

[3]School of Computer Science and IT, Jain deemed to be University, Bengaluru, India

[4]Department of Mathematics, Chaudhary Charan Singh University, Meerut, India

[5]Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India

[6]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia

Correspondence
Saru Kumari, Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh, India.
Email: saryusiirohi@gmail.com

Abstract

Recently, The Internet of Vehicles (IoV) concept is becoming very popular due to sharing of the data between vehicles and the infrastructure. The sharing of data is very important for enhancing vehicular services, but at the same time makes IoV vulnerable for security and privacy issues. The smart and interconnected vehicles produce sophisticated services for transport authorities, car manufacturers, vehicle owners, and other service providers. IoV are very vulnerable to malicious attacks due to its self-organizing nature and the open source nature of its implementations. This exposes the smart and interconnected vehicles to a variety of privacy and security threats, such as a remote hijacking or location tracking of vehicles. Thus, the security for IoV environment is critical. Blockchain technology has been recently used for cybersecurity due to the robustness and integrity preserving nature of its design. This review article provides a detailed survey of existing work in the literature to secure IoV through blockchain techniques such as security, privacy, reputation, distributed, decentralized, data sharing, authentication, and trust-based approaches. The paper presents the detailed discussion and analysis of these blockchain techniques to secure IoV. In addition, we present the gaps and research challenges identified from the existing research works. This provides work directions for future research in blockchain techniques to secure IoV.

1 | INTRODUCTION

With the rapid growth of the Internet of Vehicles (IoV) and the automobile industry, the vehicles produce various kinds of data using onboard devices. The vehicles share and collect the data for improving driver safety and obtaining a better intelligent transportation system with high quality of service.[1] However, several privacy and security challenges exist in order to share data in the IoV. At the same time, the vehicles are not able to upload the data to the infrastructures that are situated on roadside units ((RSUs) with centralized management architecture due to the possibilities of data manipulation and a single point of failure. The Peer-to-Peer (P2P) data sharing concepts can be applied to the vehicles to resolve the problems of centralized management, but we still face the data issues without proper protection and authorization in the architecture. These challenges affect the vehicle data circulation, even forming a data “island”, and hence delaying the future development in IoV.[2]

Autonomous self-driving capabilities and features in smart vehicles continue to increase. As a consequence, security and privacy breaches will result in accidents and threaten the lives of road users. Due to significant processors and energy constraints, sensor networks, and state of art mobile networks for vehicles are currently lacking configuration support for standard IoV devices. Furthermore, in autonomous vehicles, instead of a one-time initial configuration, efficient real-time authentication is needed because the vehicle must consistently authorize several vehicles on the road. The Blockchain (BC) provides a decentralized Framework for Real Time Applications to enable and ensure the secure communications between two vehicles and other acts in intelligent transportation systems. Blockchain also enables the privacy and performance of the new proposed techniques in terms of availability, costs, integrity, execution time, and immutability. Due to the above reasons, the blockchain scheme is integrated with IoV and has attracted various researchers due to its anonymity, trust characteristics of blockchain, and decentralization.[3] The blockchain introduces the trusted, secure, and the decentralized intelligence-based transport ecosystem for solving vehicle data-sharing issues.[4] In Reference 5, the blockchain-enabled data-sharing approach that was devised provides the capability to address the control challenges connected with the stored sensitive data. This is based on built-in autonomy and immutability properties of the blockchain. In Reference 6, the blockchain-distributed method was devised for distributing the patient data and employing the blockchain network for creating the prediction model. A privacy-preserving data platform based on blockchain has been proposed in Reference 7 in which the data were stored and encrypted in the blockchain federation where the data user gets the decryption key from the data owner.

With the recent advancement of the Internet of Vehicles (IoV), many vehicles need to get into this vast IoV system, but the traffic to be dealt with and measured is enormous. Simultaneously, with the expansion of traffic load on unified frameworks bottleneck is an issue.[8,9] In addition to the expensive and complex designing procedures, the focal server could be the bottleneck of the whole framework. If the server comes up short, it might break the entire framework. Moreover, it is hard for various suppliers to ensure interoperability and similarity among systems.

Figure 1 depicts the blockchain-based Internet of Vehicles security architecture. Figure 1 shows the overall architecture for the blockchain-based Internet of Vehicle security. Vehicles connected in the blockchain network either act as “miner” nodes or “peer” nodes. The blockchain network contains “n” number of miner nodes and “m” number of peer nodes. The miner node will verify if any new node joins in the blockchain-based internet vehicles security network. Peer nodes in the network only use the service offered by a blockchain network. For example, in a blockchain-based inventory network, the board, record keeping, and provenance following become simple as the item data can be obtained through

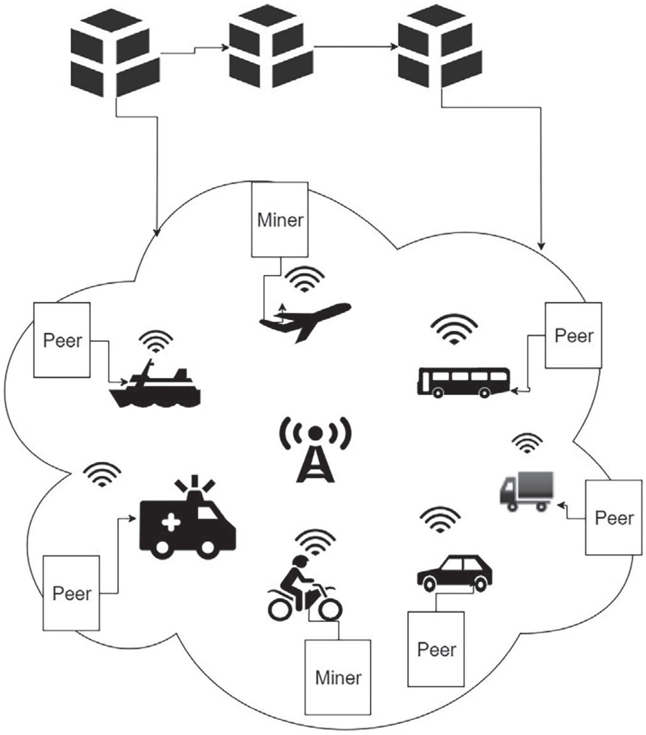

FIGURE 1 The architecture of blockchain-based Internet of Vehicles security

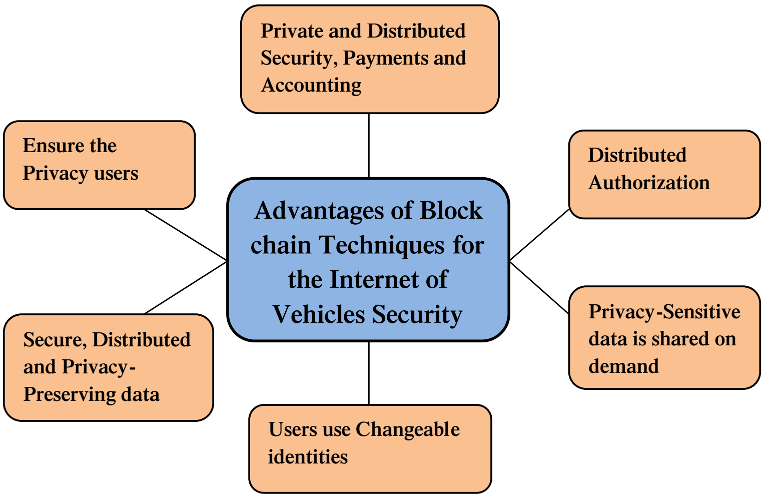
Private and Distributed Security, Payments and Accounting
Ensure the Privacy users
Distributed Authorization
Advantages of Block chain Techniques for the Internet of Vehicles Security
Secure, Distributed and Privacy-Preserving data
Privacy-Sensitive data is shared on demand
Users use Changeable identities

FIGURE 2 The advantage of block-chain techniques for the Internet of Vehicles security

implanted sensors and radio-frequency identification labels. The historical backdrop of an item directly from its start to where it is in the here-and-now can be followed through blockchain. Figure 2 depicts the advantage of Block-chain techniques for the Internet of Vehicles security.

The primary contribution of this paper is to review various existing blockchain techniques for IoV security. As per our literature review, there is no existing work that reviews the blockchain-based methods for IoV security. We categorized the existing blockchain-based security methods for IoV into security, privacy, reputation, decentralized, data sharing, and authentication-based approaches then analyzed the research gaps. The survey is also conducted from the timeline, tools used by the researchers, and performance evaluation metrics used in the experimentation perspective. Moreover, the adopted average execution time is considered for the performance evaluation of suggested blockchain in vehicles. The limitations of the existing blockchain-based methods related to IoV security are analyzed and specified as the research gaps. This will inspire future research in the extension of effective blockchain techniques to secure IoV.

This paper is organized as follows: Section 2 discusses the security threats from IoV perspective. Section 3 elaborates the review of blockchain methods presented in the literature classified by security-based, reputation-based, distributed-based, decentralized-based, data sharing-based, authentication-based, trust-based, and other techniques. Section 4 discusses the analysis of the techniques based on year of publication, toolset, techniques, and performance metrics. Section 5 discusses the research gaps and open issues. Finally, Section 6 presents the conclusion remarks.

2 | SECURITY THREATS IN IOV

Cybersecurity-related threats are an important issue.[10-29] Similarly, there are several possible security attacks in IoV that can be classified based on security requirements: Authentication, Confidentiality, Integrity and Availability.[30-32]

2.1 | Authentication-related attacks

"Sybil" attack: In this attack, attackers create fake nodes to create chaos in the vehicle network. In addition, a GPS deception attack is possible where the attacker sends fake GPS signals to misguide a vehicle. This attack is named based on a study of a woman with multiple personality disorder. Similarly, an attacker can claim or take different identities and use these identities to cause disruption to the normal functioning of the system. In an IoV environment, a node with multiple identities and malicious intent can damage the system by controlling the other vehicles or nodes in a given moment. Considering the dynamic and fast-moving nature of the IoV, this type of an attack is easy for the attackers to launch and cause substantial damage to IoV network.

Masquerading attacks: Classical masquerading attacks, where an attacker pretends to be one of the entities in the IoV network. This type of an attack is also called as impersonation attack. In this attack, the malicious entities act like a benign user and perform actions as if they are beneficial to the network. However, after some time they cause actions with malicious intent to confuse and misdirect the benign normal users. This attack is made possible by having multiple nodes in IoV network with same identifier. That way, the malicious user gets hold of authentic identifier and then use this ID to gain an unauthorized access to the IoV network and cause further damage.

Wormhole attack: Wormhole attack, the malicious nodes collude to misguide victim vehicles and also cause deadlocks. These types of attacks happen when an attacker tries to create bogus network links in order to control the flow of the traffic. This is possible by making the legitimate nodes believe that these bogus links result in the best route to reach the destination.

2.2 | Availability-related attacks

Denial of Service attack: In Denial of Service attacks, the attacker sends fake requests to genuine nodes and disrupts the vehicular communication. In this type of attack, the attacker bombards the genuine server/host node with request such that it will not be able to serve the genuine requests from the other nodes in IoV network, resulting in disruption of the service. In the distributed denial of service attacks, the attacker uses multiple compromised systems such as bot (zombies) to flood the network from many different directions and cause severe damage to the IoV system. As a result, the vehicles will not get the required data such as directions and road status and the vehicle network may end up standstill.

Channel Inference Attack: In channel inference attacks the malicious attacker jams the communication channels and disrupt the communication. This attack utilizes the limited and transmission power bandwidth nature of IoV systems to collapse it.

2.3 | Integrity-related attacks

From an integrity perspective, the malicious nodes modify the routing information to misguide the genuine vehicles in the network. By integrity, we mean that data that have been transmitted from source node is not modified when it is received at sink node. In such type of attacks, attacker somehow enters IoV system and accesses the packets that are being sent in the IoV network, modifies them and then send to the sink node. Following are the possible types of Integrity-related attacks.

Man in the Middle (MITM) Attacks: In this type of an attack, the malicious entity obtains confidential information such as key or data between the sender and receiver. This is a very critical attacker since the vehicles can be fooled as if the information is coming from the genuine node in the IoV network.

Forgery attacks: In this type of attack, the malicious entities fakes to be a user device in the IoV network and start controlling the IoV system by modifying the control packet as per its will.

2.4 | Confidentiality and privacy-related attacks

Eavesdropping attacks: From confidentiality and privacy perspectives, the IoV networks are prone to eavesdropping attacks. These attacks are difficult to protect due to their passive nature. In this type of passive attack, attacker passively sees all vehicles and the user data passing through it.

Reconnaissance attacks: In this type of attack, the attacker will be gathering information about IoV network for use in a future attack.

3 | LITERATURE SURVEY

In this section, we review different blockchain approaches in IoV. Figure 3 illustrates the classification of distinctive blockchain techniques. Here, different techniques, such as security-based approaches, privacy-based approaches, reputation-based approaches, distributed-based approaches, decentralized-based approaches, data sharing-based approaches, authentication-based approaches, and trust-based approaches, are described to provide clarity of the blockchain techniques to secure IoV. We believe that the limitations of these methods will motivate researchers to develop novel methods for blockchain techniques.

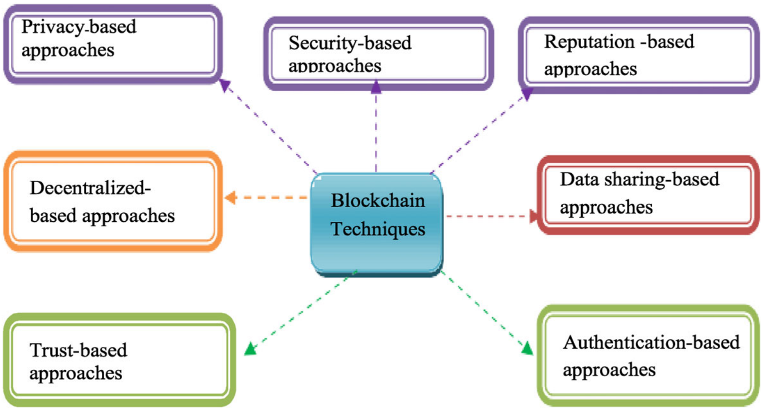
Privacy-based approaches
Security-based approaches
Reputation -based approaches
Decentralized-based approaches
Blockchain Techniques
Data sharing-based approaches
Trust-based approaches
Authentication-based approaches

FIGURE 3 Categorization of blockchain approaches in IoV

Mendiboure et al proposes the importance of blockchain framework for IoV applications in Reference 33. They indicate that in order to make IoV a reality, several security and operational requirements should be considered and that Blockchain can play an important role in addressing these issues to implement an IoV concept widely. While there are challenges to integrate Blockchain technology with IoV, studying them and solving these challenges are important to realize the vision of IoV.[33]

As per our literature review, any survey paper does not exist on the Blockchain Techniques for Internet of Vehicles security. However, there are survey works on how blockchain is used in IoV for Intelligent Transportation Systems,[9] blockchain for IoT security,[34] blockchain-based applications in Internet of Vehicles,[33] blockchain for IoT,[35] and blockchain and edge computing for IoV.[36]

3.1 | Classification of blockchain techniques

In the following sub-sections, we illustrate the specific research works that make use of different blockchain approaches for IoV. The analysis of different blockchain techniques employed for IoV is also described

3.1.1 | Security-based techniques

In this subsection, we review the security approaches employed for blockchain in IoV. Vehicles are secured using blockchain. Figure 4 shows how a blockchain secures vehicle to vehicles communications or vehicles to public infrastructure.

Chaudhary et al developed Blockchain-enabled secure energy trading (BEST) for Electrical Vehicles (EVs).[37] In this framework, the blockchain was utilized for validating EV requests in a distributed way to ensure the resilience over single-point failure. In this case, the miner nodes were chosen for validating the requests based on the time of stay, connectivity record, energy requirements, and dynamic pricing. Besides, software-enabled networking is employed as a network backbone for sending EV requests to the global software network controller.

Iqbal et al developed the characterization of the vehicle malware as well as the security architecture for protecting the vehicle from the malware.[38] This architecture employed multiple computational platforms and used a virtualization approach for limiting the attack service. They designed a real-time operating system for controlling the functionalities of a vehicle and other operating systems for non-critical functionalities. The security architecture also describes the group of components for preventing malicious activities and performing policing (monitor, control, and detect).

Li et al presented Fog Computing-based Secure Demand Response (FSDR) for the Internet of Energy (IoE) based on Access Control Encryption and consensus against the collusion attacks.[39] In the FSDR, the node was re-established as the sanitizer for transferring the design response (DR) strategies and the encrypted energy states in a random manner. Liu et al developed blockchain-driven data and energy coins using consensus, where the data contribution frequency and the energy contribution amount were applied for achieving better system performance.[40] In addition, they also presented the security solutions to secure vehicular interactions in the Electric Vehicles Edge and Cloud Computing.

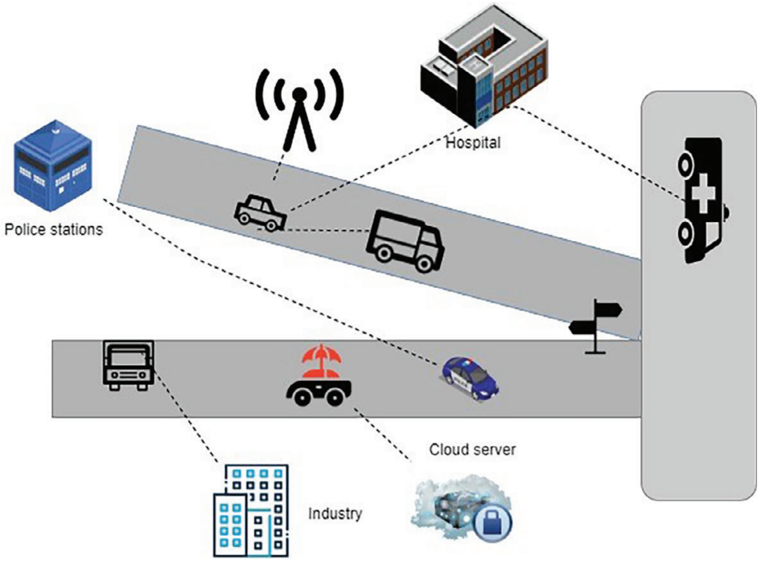

FIGURE 4 Vehicles security using blockchain

Kim et al developed a secure EV charging system based on blockchain, addressing the security issues in the charging systems.[41] This charging system ensures a mutual authentication, better forward secrecy, the security of a key, and also provides effective charging. Qian et al, designed a method to assess the feasibility of the private BC approach to solve security issues, such as high processing time or preserving the integrity, confidentiality, and authenticity.[42] In this framework, in-vehicle networking systems, such as switches, and central (or connected) gateways (cGW) were considered. In this case, switches and cGW are the BC nodes in which the BC consensus protocols keep all nodes synchronized to each other.

Singh and Kim developed Intelligent Vehicle- Trust Point (IV-TP) for the communication of vehicles from IVs based on Blockchain technology.[43] In this approach, the communication data provide the reliability and the security of the network. Ao et al developed an approach to provide the secure key management inside the heterogeneous network.[44] In this case, the SMs play a vital role in vehicle departure information retrieval, encapsulating block to the transport keys. After that, the rekeyed vehicles were executed in the identical security domain. In the initial phase, the novel Group Key Management (GKM) approach was introduced, which is based on Leaving Probability (LP) of vehicles for vehicular communication systems (VCS). This factor was utilized for achieving the efficient rekeying scheme, and the limited rekeying costs. In the second part, the BC concept was established for simplifying the distributed key management in the heterogeneous VCS domains.

Rowan et al developed a secure inter-vehicle communication system based on side channels.[45] This approach was utilized for verifying the position and finding the vehicle being communicated with, and it incorporates that vehicle identifier in cryptographic set up exchanges. Huang et al presented a decentralized security approach based on the lightning network and the smart contract in the BC ecosystem.[46] The overall procedure of the developed model involved scheduling, registration, charging, and the authentication phase. Here, the security scheme was integrated easily with the current scheduling approaches for improving the trading security between charging piles and electric vehicles (EVs).

Rathee et al developed a security mechanism to connect the autonomous vehicle services approach based on the BC technique.[47] The IoT devices or the vehicles were traced and recorded within the BC for providing the transparency and secrecy of the cab drivers and the customers. Zhang et al presented the security architecture of vehicles using edge computing and BC.[48] This architecture is comprised of three layers: edge computing, perception, and the service layer. The perception layer is introduced to utilize the security of the vehicle data in the transmission process based on the BC approach. The edge layer generates the computing resources, and the edge cloud services to the perception layer. The service layer employs the integration of traditional cloud storage and BC to ensure the security of the data.

Xu et al introduced secure networking computing services for lightweight clients using Blockchain.[49] In addition, blockchain was established for providing security services. Subsequently, the smart contract was introduced to check the validity state of lightweight clients as on-chain services. The method failed to make the service provider employ blockchain, and they utilize IoT-based feedback for obtaining the best trade-off, availability, and best system performance.

Lapets et al[50] designed a multi-party computation (MPC) protocol to allow groups of co-operating users with minimal expertise; there are no specialized resources needed apart from the contribution of individual participants.[50] This system was mainly used for Boston Women's Workforce Council. Bogdanov et al designed the MPC approach using small primitive components.[51] The composability of security notions plays a significant role in this system in order to deduce the properties of complex protocols. Then, the weaker notion of privacy was introduced as the passive security model for converting the private protocol into the universally composable protocol.

Micciancio and Tessaro developed a method for securing MPC.[52] The feature in this framework allows to specify the protocols in a manner that is independent of time, through the simplified cryptographic protocols. From a level of notation perspective, the protocols were described by the systems of mathematical expressions.

Zhu et al designed a method based on both space and time parameters.[53] Here, the protocol, named WRK, was introduced to address various significant cryptographic and programmatic challenges. Then, the staged execution model was established based on the combination of dynamic program instrumentation. Rahman et al developed secure IoV for handling the transportation ecosystem of the dynamic crowd.[54] This approach allowed the personalized as well as the location-driven vehicle IoT data in order to save the IoT data in off-chain and blockchain repositories. Table 1 summarizes the security challenge and its applications for the security-based blockchain techniques.

Kim et al developed Enhanced Blockchain-enabled IoV (EBIoV) to protect the connected car from attackers.[55] Here, this approach was designed on the basis of decentralized network and employed Blockchain Governance Game strategy to improve the security of the connected car. For the security developments, the optimization was introduced to reserve the honest nodes. Yin et al developed bidding mechanism for contributing the resources for better vehicles. Then, the time window-enabled approach was introduced for managing tasks between the vehicles.[56] Finally, the blockchain framework was designed for achieving secured information through the smart contract in IoV.

Saied et al developed collaborative schemes for key establishment to reduce the needs of previous security protocols.[57] The constrained device delegates their heavy cryptographic load to the less constrained nodes in the neighborhood using spatial heterogeneity in IoT. Arora and Yadav developed an authentication-based secure data transfer approach in

TABLE 1 Security-based techniques security challenge and its applications

S.No	Method	Security challenge/limitations	Application
1	Blockchain-based secure energy trading scheme	Single point of failure, and communication/computation overheads on the network resources.	Energy trading in SDN-enabled intelligent transportation system
2	Fog Computing-based Secure Demand Response	Demand response is dangerous, and node can be easily attacked by a Distributed denial of service of attack.	Internet of Energy
3	Electric Vehicles Cloud and Edge Computing	Because of the information affectability and setting multifaceted nature, vehicular applications stand up to genuine security issues.	Contexts-aware vehicular applications
4	Electric vehicle based on blockchain	Electric vehicle charging frameworks are defenseless to a disseminated refusal of administration and favored insider assaults when the focal charging server is hacked.	Electric vehicles charging
5	Intelligent vehicle-trust point	Lack of trust, information exactness and quality of correspondence information in the data transmission link.	Intelligent vehicle communication
6	Lightning network and smart contract	Key can be easily compromised by the attackers.	Electric vehicle and charging pile management
7	Autonomous vehicles services framework	Malicious clients in the web of vehicles may misdirect the entire correspondence where gatecrashers may bargain savvy gadgets to execute a malevolent ploy.	Online cab booking
8	Blockchain-based secure service provisioning mechanism	Blockchain-based plans typically have low throughput and high assistance idleness issues and take little thought of essential data refreshing just as the lawfulness approval of the various service	Lightweight clients from insecure services in-network computing scenarios.

network-based blockchain technology.[58] Initially, the blockchain protocol was developed for security in P2P transfer of the bitcoins, but its performance has opened doors for its implementation in less secure areas.

Balasubramaniam and Sathyanarayanan developed a holistic approach to improve the connected vehicle security using the blockchain.[59] In addition, this approach focused on security services with intrusion protection throughout the life cycle of the vehicle, which ensures the end-to-end protection. Li et al developed a secure energy trading system, termed as an energy blockchain for addressing security challenges.[60] This approach was utilized in the general scenarios of the P2P energy trading system using the trusted intermediary. Then, the credit-driven payment scheme was introduced for supporting fast, as well as frequent, energy trading.

Davi et al designed blockchain-enabled architecture using a shared ledger within a car from which every electronic control unit (ECUs) acts as the miner and shares their information with the other ECUs.[61] Here, this architecture enhances the integrity of information for forensics.

Sharma developed an energy-efficient transaction model using blockchain technology in IoV.[62] This approach was utilized for reducing the number of transactions required for updating the ledgers on IoV. The main aim of the developed model is to mitigate the burden of network from the several blockchain transfer operations while the maximal available energy was conserved. To achieve this, the distributed clustering model was introduced for energy conservation.

3.1.2 | Privacy-based techniques

In this section, we review the IoV security methods proposed in literature using the privacy-based techniques. Figure 5 depicts the vehicle's security using privacy-based techniques.

The research work based on the privacy approaches for blockchain in IoV is discussed as follows: Gao et al developed a blockchain-enabled privacy preserved payment approach for Vehicle-to-Grid (V2G) networks.[63] This approach is utilized for sharing the data with the secure user information. In this case, the data and registration maintenance were introduced based on the blockchain approach for enabling payment auditing by users. Xu et al modeled the edge computing-based computation offloading approach to tackle privacy leakage problems with privacy preservation.[64] After that, the Vehicle-to-Vehicle (V2V) network based on vehicle routing was designed for obtaining the origin vehicle, where the computing task was assigned at the destination vehicle.

Baza et al developed and distributed firmware updates for Autonomous Vehicles (AVs) subsystems, leveraging smart contract, and blockchain technology.[65] Here, the consortium of blockchain with various AVs are utilized for ensuring the integrity and the authenticity of firmware updates. Kang Liu et al developed a secure, decentralized data trading and debit-credit system for IoV using blockchain.[66] In this scheme, the authors designed mechanism to encourage borrowing and lending among vehicles by a motivation-based debit-credit mechanism.

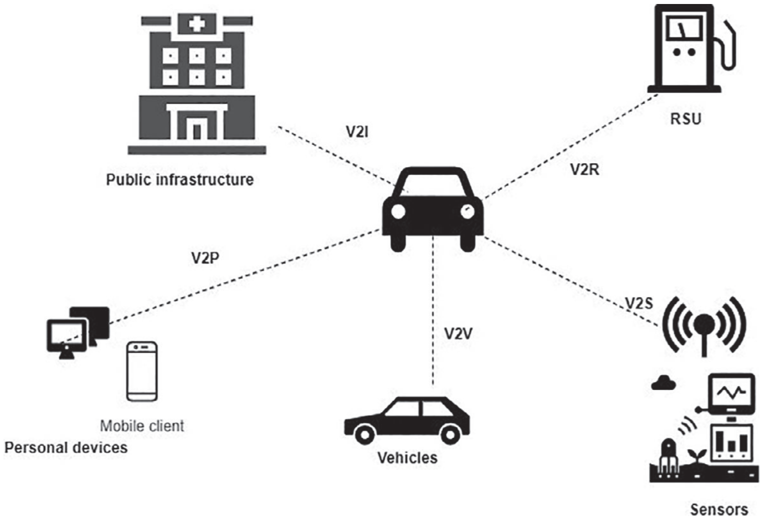

FIGURE 5 Vehicles security using privacy

TABLE 2 Privacy-based techniques security challenge and its applications

S.No	Method	Security challenge	Application
1	Blockchain-based privacy-preserving payment mechanism	Reliability and effectiveness of exchanges are the main problem in the Vehicle-to-Grid Networks. The private blockchain provides better scalability, but it will not provide better reliability of the transaction, since it will add the transaction in ledger without verifying whether the transaction is reliable or not.	Vehicle-to-Grid Networks.
2	Blockchain-based Firmware Update	By controlling the usefulness of the subsystems through the establishment of contaminated variants in the firmware, an assailant can effectively hack autonomous vehicles and completely/in part get to them, for example to include the vehicle in mishaps purposely, which may prompt sensational harms and slaughter individuals	An automatic software update in autonomous vehicles
3	Blockchain-based certificate revocation scheme	A pseudonym certificate is renounced if the endorsement proprietor indulges in harmful practices.	Vehicular communication systems

Asuquo et al presented Location-Based Services for Vehicular and Mobile Communications.[67] Lei et al discussed a blockchain-based certificate revocation scheme for VCS.[68] The proposed Blockchain structure permits the public key infrastructure by effectively setting the appropriate certificate revocation list (CRL) size. The authors have demonstrated that the Blockchain-based scheme is proficient in packing the size of CRL altogether. Besides, by breaking down the message handshake methodology among foundations and vehicles in VCS, the Blockchain gives a circulated system structure. The after effects of message overheads between testament renouncement conspire to show that the Blockchain-based plan discharges the correspondence trouble by lessening the general number of communicating messages. Table 2 summarizes the privacy-based blockchain techniques for security challenges in IoV and its applications.

Jiang et al presented a cloud-based authentication and key agreement protocol by integrating passwords, biometrics, and smart cards to ensure secure access to both cloud and AVs,[69] and integrated an authentication and key establishment protocol.[70] However, they do not involve blockchain in their solution approach.

3.1.3 | Reputation-based techniques

This section describes the reputation-enabled approaches in blockchain to provide security in IoV. Khelifi et al modeled reputation-enabled blockchain mechanism for securing cache in a vehicular environment and improved the trust between the consumer vehicles and cache stores.[71] This framework was based on the blockchain network, and comprises of cache store to increase or decrease reputation value based on server content. The developed approach is independent of the deployment cache placement policy.

Kang et al modeled the two stages in their soft security enhancement solution, such as miner selection and the block verification stages.[72] In the first phase, the reputation-enabled voting approach was introduced for the secure miner selection. This framework was utilized for computing candidate's reputation based on both recommended opinions and past interactions from the other vehicles. The candidates with maximum reputation were chosen to be the standby and active miners. In the second phase, the internal collision was prevented by active miners. Then, the contract theory was introduced for modeling the interaction between two miners in which the delay and the block verification for security was considered.

Yang et al developed the novel reputation system based on BC techniques for the data credibility assessment.[73] In this framework, the vehicles rate the received messages by observing the traffic environment and enter these ratings into the block. Every block was chained to the existing one by storing the hash value of the previous block. After that, the temporary center node was selected from the vehicles to broadcast the rating block.

Wang et al presented blockchain-enabled secure incentive scheme to deliver the energy in vehicular energy networks (VEN).[74] Initially, the permissioned energy blockchain system was introduced for implementing energy delivery services securely using cryptocurrency and distributed ledgers. Then, the protocol named Proof of Reputation was established to reach the consensus efficiently in blockchain. Consequently, the incentive model was employed to improve the EVs utilities.

Liang et al reported micro-blockchain-based interruption identification (MBID) to powerfully arrange interruption identification procedures for Internet of vehicles.[75] Specifically, in MBID, a smaller scale blockchain design was proposed to gather nearby interruption tests that can be used to build interruption identification procedures fit for the present state.[75]

Park et al proposed a motivating force plot consolidating with bitcoin on vehicular ad hoc networks (VANETs) to animate vehicles emphatically, helping out different hubs and to remunerate their endeavors.[76] Because of the security highlights of the bitcoin framework the impetuses for volunteer vehicles are remunerated by methods for bitcoin, which can be globally utilized as genuine money. In such a case, the decency to a message sender is ensured by utilizing multiset exchange with the goal that a message handing-off vehicle can get the motivating forces just if the vehicle complete the message handing-off to a goal.[76] Table 3 summarizes the security challenges and applications in IoV for the reputation-based blockchain techniques.

3.1.4 | Distributed-based techniques

The research works in the literature that utilizes the distributed-based blockchain approaches that are discussed in this section. Dorri et al presents blockchain-driven architecture for protecting the privacy of the users, and to improve the security of the vehicular ecosystem.[77] Wireless remote software updates, another emerging service such as dynamic vehicle insurance fees, were employed for illustrating the efficacy of security architecture.

Stanciu modeled BC-enabled distributed control system using the IEC 61499 standard.[78] Here, the Hyperledger Fabric was chosen as a BC solution in which the function blocks were executed as the smart contracts on the supervisor level. The combination with the edge nodes was done based on micro-services architecture. Jiang et al developed the model for outward transmission of vehicle BC data.[79] Here, several types of nodes, such as roadside and vehicles for vehicle networks, defined to form various sub-BC networks for IoV networks. The method failed to use traffic among the vehicles, and hence the channel reliability of cellular networks suffered.

Li et al designed the architecture for blockchain-driven security for cloud storage distribution.[80] In addition, the genetic algorithm was introduced for solving a file block replacement issue among the multiple data centers and users in the distributed cloud storage field. Sharma et al developed an approach by integrating blockchain with ad hoc vehicular networking for sharing the network resources with maximal reliability, security, and trust based on distributed access control.[81] Thus, this framework is utilized to share the information between the connected vehicles. Saini et al developed permissioned blockchain network for the connected vehicle network with various layers.[82] This approach ensures highest security to RSUs authorities. In this approach, the priority vehicles were able to query the trust position values and then the path movement was accessed from the source to the destination.

Li et al developed a lightweight blockchain system, NAMED LightChain. This approach is resource efficient and is appropriate for the power-constrained Industrial Internet of Things (IIoT) areas.[83] In addition, the Green Consensus mechanism called Synergistic Multiple Proof was introduced to stimulate the co-operation of the IIoT devices. Sharma designed vehicle network architecture using blockchain in Smart City context.[84] This approach resulted in the secure and reliable architecture, which operates in the distributed manner for constructing the novel distributed transport management system.

Ramaguru et al developed Real-time Blockchain for IoV to ensure authentication and maintain secure communication between vehicles.[85] In addition, the smart contracts-enabled vehicle services, such as vehicle servicing slot payment and

TABLE 3 Reputation-based techniques security challenge and its applications

S.No	Method	Security challenge	Application
1	Reputation-based blockchain	The reputation scheme may get influenced in various situations, from various system levels.	Named Data Networking caching application
2	Blockchain-based reputation	The destination vehicle has to verify that the received data have not been modified by the malicious vehicles in the network.	Data credibility assessment in vehicular networks
3	Reliable incentive scheme using bitcoin	Payment framework makes it easy to control blockchain by an attacker.	Cooperative vehicular network services

booking, automatic toll payment, vehicle insurance renewal, fuel payment and so on can be realized. Here, the developed model supports the native crypto currency for payments in the network.

Sharma et al developed Distributed Blockchain-Based Vehicular Network Architecture for Smart City.[86] The Block-VN model permits vehicles to find and share their assets to make a system of vehicles on which they cooperate. Awais et al modeled secure and decentralized frameworks for vehicular correspondence to keep IoV away from the security dangers and low conveyance paces of the consolidated framework.[87] This framework disperses attack messages through the decentralized database for various situations to stay away from a crash. Additionally, they utilized blockchain to verify the sender of a notification message through the data collected from every vehicle. The high precision rate demonstrates that the framework is effectively recognizing malicious vehicles and ordinary vehicles.

Hammi et al developed the decentralized system, termed bubbles of trust for ensuring robust authentication and identification of devices.[88] This framework relied on the security advantages provided by the blockchain (BC) to create secure virtual zones in which things identified and trusted each other. Angin et al presented an approach for the Internet of Things (IoT) systems, which introduced tamper resistance and transparency into data retrieval and storage in IoT networks.[89] This solution is based on the applications of BC for providing data security guarantees and decentralized device authentication.

Yang et al developed a decentralized trust management framework using BC techniques in IoV.[90] In this framework, the vehicles may validate received messages from the neighboring vehicles based on the Bayesian Inference model. Then, the vehicles generate the rating for each message source vehicle based on the validation result. Subsequently, the RSUs compute the trust value of vehicles and pack the data into the block. After that, every RSU adds their blocks to the trust BC, which was maintained by all RSUs.

Dwivedi et al modeled a hybrid approach that integrates the advantages of the public key, private key, BC, and various lightweight cryptographic primitives.[91] Then, the patient-centric access control was introduced in order to maintain medical records privacy and security. The proof of the work approach was employed by Abubaker et al to validate the Demand Response (DR) events.[92] This approach provides real-time mechanism supervision and real-time monitoring of the end-user. In addition, Autonomous Vehicles (AVs) with the blockchain mechanism are introduced to provide security services to the end-user. In addition, The Peer to Peer (P2P) car-sharing mechanism was employed for removing the need for any bank or any other reliable authority.

Liu et al developed BC-enabled Mobile Edge Computing architecture to provide video streaming in a distributed and secure manner.[93] In addition, the series of smart contracts were used for enabling self-organized video transcoding and the delivery service without using the centralized controller. After that, the users, Small Base Stations, and the Video Providers (VP) adjust their strategies using transactional information on BC. Finally, an iterative approach was introduced to tackle the video transcoding and the delivery issues. Table 4 summarizes the security challenge and its applications in IoV for the distributed-based blockchain techniques.

TABLE 4 Distributed-based techniques security challenge and its applications

S.No	Method	Security challenge	Application
1	Blockchain-based distributed method	Proposed method does not consider about client security—for instance, they resort to trading all information of the vehicle without the proprietor's consent or uncover confidential information to the requester.	Automotive security and privacy service for smart vehicles
2	Blockchain-based distributed control system	Challenges related to Security and protection of client's information, and specific necessities concerning individual information security.	Vehicular communication systems
3	Distributed Blockchain-Based Vehicular Network Architecture	The issue of choosing the criteria to secure conventional vehicles.	Smart city
4	Blockchain-enabled Mobile Edge Computing	Because of the constrained figuring capacities, current blockchain-based video frameworks cannot empower video transcoding, which changes a video starting with one form then onto the next rendition on the fly to discharge the enormous weight of the capacity and data transmission.	Video streaming application

3.1.5 | Decentralized-based techniques

Odiete et al presented cowry, the platform to publish metadata describing the available resources.[94] Here, the published resources, such as filtering and fast search were considered. The major contribution is the fully decentralized architecture that integrates the blockchain and the traditional distributed dataset for gaining additional features, such as retrieval of the metadata stored and efficient query on blockchain.

Skarmeta et al developed distributed approach for controlling the access to its sensitive IoV information.[95] Thus, this approach was implemented with the consideration of severe constraints of previous smart objects with respect to processing and communication power.

Abdmeziem et al developed decentralized and batch-enabled GKM protocol for securing multicast communications.[96] This protocol was very simple and it mitigates the rekeying overhead triggered by the membership changes in the mobile and dynamic groups, and guarantees both the forward and backward secrecy.

3.1.6 | Data sharing-based techniques

The data-sharing techniques employed in the blockchain as it relates to IoV security are elaborated in this section. Kang et al modeled secure Peer to Peer (P2P) data sharing systems in vehicles.[97] The smart contract technology and consortium blockchain were introduced for achieving secure and efficient data sharing and storage. Additionally, the reputation-enabled data-sharing approach was introduced with three weight subjective logic model to obtain the accurate reputation management of high-quality data sharing from the vehicles.

Brousmiche et al addressed the issues of sharing and securing the vehicle's data over consortium BC.[98] They designed the hybrid cryptographic protocol for securing the vehicle's data between the stakeholders. Zhang et al presented a BC-enabled secure data sharing system to tackle both the privacy and security issues.[99] In this case, the announcement messages were stored by BC. This framework is utilized to prevent the fake messages.

Pouraghily and Wolf developed the protocol, named Ticket-enabled Verification for defining two logical entities: transaction verifier and contract manager.[100] This framework limits the requirement for the high-performance embedded systems and mitigates the networking and processing overhead.

Luong et al developed optimal auction for edge resource allocation based on deep learning.[101] The Multi-layer neural network architecture was designed based on analytical solution of optimal auction. Here, the neural network initially performed monotone transformations of miners' bids. Later, the conditional payment and allocation was computed for miners, and then the valuations of miners were used for adjusting the parameters in neural networks for optimizing loss function.

Mahmood et al developed Efficient Key Management (EKM) for the multiparty communication-enabled scenarios.[102] The session key management protocol was introduced by applying the symmetric polynomial for the group members, and group head acts as the responsible node. Here, the polynomial generation approach utilized secure hash function and security credentials.

3.1.7 | Authentication-based techniques

This section elaborates on the authentication approaches in the blockchain using various methods. Wazid et al modeled the lightweight Authenticated Key Management Protocol (AKM-IoV) for dealing with secure communication from several entities in the IoV platform.[103] AKM-IoV comprises of three steps (a) AKM between vehicle and fog server, (b) AKM between RSU and fog server, and (c) AKM between the cloud server and fog server. In all three phases, after the mutual authentication, the communicating parties establish the session keys for secure communications. Wang et al developed a BC-based approach in IoV. Here, the BC framework was devised for designing a key distribution mechanism.[104] The BC ledger techniques were employed for a new node joining mechanism, and the BC consensus was introduced for finding a new vehicle identity authentication mechanism.

Sharma and Chakraborty designed the architecture for the vehicular information system based on blockchain for maintaining consensus between the distributed services in order to ensure privacy preservation, data integrity, and the vehicle authentication.[105] This framework was designed to manage massive scale IoV data. The local caching scheme was introduced for avoiding large transaction time. Pal et al developed the blockchain technology which was utilized for the

IoT systems.[106] Here, the blockchain techniques removed the requirement of third party for validating transactions over network. Here, the blockchain also included the key management systems for the Blockchain Public Key Infrastructure and bitcoin currency wallet.

Hernandez-Ramos et al developed lightweight authentication and the authorization approach for supporting the smart objects during the life cycle.[107] Li et al proposed privacy-preserving protocol to ensure the announcements are reliable. The proposed protocol is efficient and effective in the untrusted VANET environment.[108] Based on the author's simulations, they found out that total time of announcements per user is very efficient than other protocols. The incentive mechanism of the protocol also encourages users to be active in the communication. Due to the Blockchain techniques in their approach, they noticed that security is enhanced by observing announcements and transactions that can be traced only by the Trace manager.[108]

Sharma et al designed a novel vehicular data framework utilizing Blockchain innovation to keep up an agreement among conveyed specialist co-ops to guarantee information honesty, vehicle verification, protection safeguarding, and consistent access control.[109] This decentralized blockchain structure is exceptionally reasonable to oversee the enormous scale of information. The constraint of longer exchange time can be kept away by receiving the proposed procedure that may be valuable in profoundly unique IoV conditions.[109] Ferdous et al proposed an autobiography of smart cars leveraging blockchain technology to make a permanent record of each datum, called the self-portrayal of a vehicle, created inside its life expectancy.

Additionally, the authors clarify how the permanence trademark of the blockchain ensures the trust in this record. The data can be shared between one vehicle to another vehicle using the autobiography method, which provides added authentication service using blockchain.[110,111] Esposito et al proposes a novel solution for distributed management of identity and authorization policies by leveraging the blockchain technology from a smart city perspective.[112] Table 5 summarizes the authentication-based techniques security challenge and its applications from the IoV perspective for authentication-based blockchain technique.

3.1.8 | Trust-based techniques

The analysis based on different trust-based blockchain approaches for IoV security is elaborated as follows: Arshad and Javaid designed the vehicular network architecture using blockchain for the smart city.[113] This approach was introduced to eliminate problems related to the malicious nodes and selfish nodes. In this scenario, the malicious behavior of the nodes was handled based on the incentive mechanism and trust values. Fort et al developed TrustedPals to solve the secure Multi-party Computation (SMC) problem.[114] The TrustedPals is an efficient smart card-enabled implementation of SMC for any number of participating entities of the model. The security models were trusted by other processes to establish secure channels between each other.

Mendiboure et al developed an architecture, named SD-IoV for improving the resource utilization, IoV network management, and the QoS. Here, an innovative trust establishment system was also introduced based on the blockchain technology.[115] The main objective of this system is to handle application identity, application behavior, and network resource management and allocation. Sheas, and Javaid developed trust value scheme using blockchain technology for trust management and reliability in IoV.[116] Here, the trust value refers to the trustworthiness behavior of the vehicle. In addition, the credit-enabled incentive approach was introduced based on the vehicle performance.

TABLE 5 Authentication-based techniques security challenge and its applications

S.No	Method	Security challenge	Application
1	Improved authentication scheme based on blockchain framework	Fake message is being sent to the server to adulterate the traffic circumstance and influence the ordinary traffic.	Smart contract
2	Blockchain-based novel architecture for vehicle authentication and privacy preservation	Abuse of private information by the administration suppliers or harmful clients disregard the security strategy and could cause cultural misfortune	BlockAPP
3	Autobiography of a smart car	The information produced by clear vehicles does not have an appropriate system to ensure secrecy, realness, and reliability.	Smart Cars

3.1.9 | Other techniques

The analysis based on other blockchain-based techniques in IoV security is elaborated in this subsection. Ali et al developed a decentralized architecture for access control and the permission delegation of IoT, with demands on the query and event-based permission delegation.[117] Then, the Blockchain was introduced for making delegation services to be trusted, secure, decentralized, and verifiable. Lei et al presented a vital management approach for transferring the key from security managers (SMs) in heterogeneous VCS.[118] This approach adopted the BC concept and optimized the performance based on dynamic transaction collection periods. This BC structure allows the key to transfer securely in the decentralized SM network. Then, the collection period selection technique was introduced for shrinking the essential transfer time of the BC scheme. Finally, the dynamic transaction collection period was further optimized to reduce key transfer time costs.

Sharma modeled an energy-efficient transaction system for BC-based IoV. This approach was utilized for solving the ledgers to pose severe issues for vehicles by controlling the transactions optimally based on distributed clustering.[119] Liu et al presented Deep Reinforcement Learning (DRL)-enabled performance optimization for BC-driven IoV.[120] Here, the transactional throughput was reduced to address security and latency of underlying BC system, however, guaranteeing a decentralization. Here, the DRL approach was introduced for selecting the block producers and adjusting the block interval and the block size for adapting the dynamics of IoV scenarios.

Zhou et al modeled an energy-efficient vehicle based on edge and BC computing.[121] Initially, the consortium blockchain-enabled secure trading approach was introduced for Vehicle to Grid (V2G). After that, edge computing was established for improving the probability of block-creation. In this case, the computation problem was then solved by the two-stage Stackelberg leader-follower game, and the best solution was obtained from the backward induction approach.

Salem et al developed a private blockchain approach for solving integrity, authenticity, and confidentiality issues.[122] Here, in-vehicle networking was considered, which contains switches and a central gateway. Wang et al[123] developed a collaborative vehicular edge computing approach, termed CEVC. The CEVC is the centralized, physically dispersed network. This approach supported scalable vehicular services and the applications of both vertical and horizontal collaborations. The method did not consider artificial intelligence and deep learning to maximize system performance.

Bickson et al developed an approach to enable secure multi-party numerical components in the peer-to-peer network.[124] This issue arises in the full range of applications, such as distributed computation of trust and reputation, collaborative filtering, and so on, in which the computing nodes preserved the privacy of inputs when joint computation of a specific function was performed. Ames et al developed a zero-knowledge argument protocol where the communication complexity is directly proportional to the square root of the circuit size.[125] This protocol is based on a collision-resistant hash function.

Video-based security techniques have been used in the literature lately that can be used for IoV security. For example, Chang et al propose a novel video-based semantic pooling approach for attack detection[126] and through semantic representation utilizing image/video archives.[127] Luo et al propose a novel semi-supervised feature selection method for video semantic recognition that can used for the attack detection.[128] Wang et al discuss a visual saliency guided complex image retrieval model to extract events from multi modal data[129]

4 | ANALYSIS AND DISCUSSION

In this section, we discuss the survey of blockchain techniques to secure IoV using metrics such as year of publication, categorization of approaches, performance evaluation metrics, usage of toolset, and performance evaluation metrics.

4.1 | Analysis in terms of publication year

As per our analysis, more than 75 research papers are published to develop effective blockchain techniques to secure IoV. The analysis in terms of publication year is depicted in Table 6. Seventy five papers were surveyed, and the number of research papers published increasing steadily from year 2010, with the highest papers published in the year 2019.

TABLE 6 Analysis with respect to publication year

Published year	Number of research papers
2019	31
2018	6
2017	11
2016	2
2015	2
2014	3
2013	1
2010	2

4.2 | Analysis in terms of the toolset used

We also performed analysis in terms of the experimentation tools used by the researchers in these distinct research works. Figure 6 depicts the experimentation tools used by the researchers for conducting experiments for the blockchain-based techniques to secure IoV. The commonly used toolsets for blockchain are Hyperledger/fabric-chain tool, MATLAB, NS2 simulator, OMNeT++, SUMO, Crypto++, PyTorch with Python 3.6, CloudSim, C, C++, ubuntu 16.04.2, and Amazon EC2 compute-optimized instance c5. As shown in Figure 6, it is clear that the most frequently employed experimentation tool is MATLAB.

4.3 | Analysis in terms of techniques

We conducted analysis based on blockchain techniques utilized by the researchers to secure IoV. The techniques utilized for the effective blockchain approaches is shown in Figure 7. The figure reflects that 42% of the research projects utilized security-based approaches, whereas 18% of researches employed decentralized-based approach. It can be noted that 8% of researches used an approach based on data sharing, and 5% used an authentication-based approach. The distributed-based approach is utilized by 7% of researchers, and reputation-based approaches is adapted in 7% of the researches.

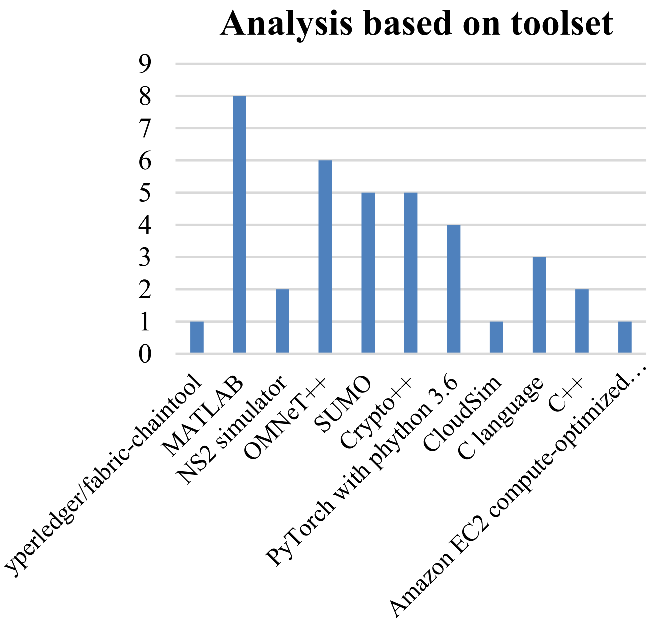

FIGURE 6 Analysis based on toolset

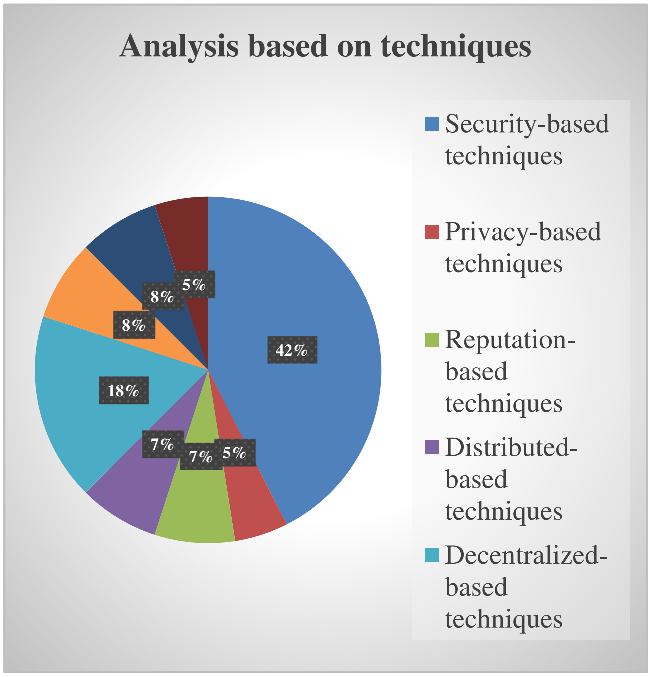

FIGURE 7 Analysis based on categorized blockchain techniques

Moreover, 5% of the researches are based on privacy-based approach. From the analysis, it can be noted that security-based methods are the most commonly employed blockchain approaches for securing IoV.

4.4 | Analysis in terms of performance evaluation metrics

In this subsection, we present the analysis in terms of performance analysis metrics to evaluate the performance of blockchain techniques to secure IoV. These analysis results are presented in Table 7. The metrics considered are time, cost, key transfer time, power, reputation value, detection rate, utility, detection accuracy, throughput, end-to-end delay, packet loss ratio, energy and network congestion. From Table 7, it is clear that the time, cost, and utility are widely preferred performance evaluation metrics in the research involving blockchain techniques to secure IoV.

TABLE 7 Analysis in terms of performance metrics

Performance metrics	Number of research papers
Time	1,2,60,68,73,75,81,82,85,88,94,95,103
Cost	55,66,73,75,83,87,116
Key transfer time	180
Power	37,50,73
Reputation value	38,41
Detection rate	38,41
Utility	38,39,51,92
Detection accuracy	43
Throughput	46,54,83,94
End-to-End delay	46,75
Packet loss ratio	46
Network congestion	68,98
Energy	62,74,81,102

TABLE 8 Analysis based on time

Range of time (s)	Number of research papers
30-40	52,82
50-60	1,60,75
60-70	73,103,114,120
70-80	2,52,68,81,85,95

Since "time" is the widely used performance evaluation metric, we conducted deeper analysis in terms of "time" performance evaluation metric. Table 8 depicts the analysis in terms of average execution time specified using four ranges such as: 30-40 seconds, 50-60 seconds, 60-70 seconds, and 70-80 seconds. From Table 8, it can be shown that works[2,52,68,81,85,95] had improved average execution time with the range 70-80 seconds.

5 | RESEARCH GAPS AND CHALLENGES

Based on our review of the blockchain techniques to secure IoV, we describe the research gaps and challenges in this section. The research gaps in the security-based approaches are as follows: The method in Reference 37 failed to consider the flow control mechanism in software-defined networking (SDN) for improving the network throughput. The lightweight design was not provided to improve the scalability in more IoE scenarios. The method[71] failed to apply IoT-enabled practical EV charging systems for the resource-constrained devices. In Reference 47, the reinforcement and deep learning were not considered to improve the system performance. Several blockchain-driven cybersecurity, such as decentralized service network securities and IoT was not considered.[25] In Reference 58, the authors failed to use centralized devices in the IoT, such as networking and the cybersecurity. The method in Reference 60 failed to consider optimal energy aggregator selection for Industrial Internet of Things (IIoT) nodes with poor or excellent credit values. A consensus algorithm was not considered in Reference 61 for improving performance and scalability. The gaps and issues identified from the privacy-based approaches are discussed as follows: membership benefit policies and cash feedback strategies are not considered for achieving anonymous transactions.[63] Real-world scenarios with various time intervals were not considered for identifying the offloading strategy and for obtaining the energy savings of the Edge Computing Devices.[64]

The limitations and gaps of the reputation-based approaches are as follows: the method in Reference 71 was not implemented in the real Named Data Networking testbed and failed to merge the cross-industry blockchain approaches, such as Hyperledger.[71] The method in Reference 38 failed to consider more weights to enhance the accuracy of the miner candidate reputation. The method failed to address the optimization problems in the second and third levels in VEN.[74]

The challenging issues of the distributed-based methods are as follows: the new-mobility friendly approach was not established to mitigate the overload. The method in Reference 67 failed to use IEC 61499 standard for the function blocks implementation to perform the required functionality to secure IoV. The method in Reference 79 did not consider the channel reliability of cellular networks and the traffic from the vehicles. The main drawback of this approach is that the high workload failed to bring several pending transactions.[83]

The gaps and issues identified by the decentralized-based approaches are discussed as follows: the method in Reference 88 failed to simulate the revocation mechanism for the compromised devices. The method in Reference 43 failed to analyze the abnormal network traffic monitoring using machine learning approaches.[43] In the method,[93] the security problems concerning malicious consensus nodes were not considered by contract theory and reputation.[93] In the method,[92] the vehicles failed to provide a comfortable service, and the available time to the customer for getting a positive rating is comparatively smaller.[92] A testable system was not considered for providing some real work security guarantees in Reference 91. Additional features are not included in the distributed model as well as their suitability for various IoT use cases in Reference 95. The method in Reference 96 failed to investigate the performance of the protocol under various mobility and the network models utilized in the real IoT test-beds.[96]

The issues of data sharing-based methods are explained as follows: the transaction rates and the volume for scalability issues were not analyzed in Reference 98. The method in Reference 75 does not consider Ethereum in order to improve the throughput of the system. Multiple edge computing resource units are not considered to improve the system performance in Reference 101. The method in Reference 102 failed to implement EKM in Ubiquitous to Internet of Thing (U2IoT).[102]

TABLE 9 Summary of gaps/challenges

S.No	Parameters	Gaps/challenges
1	Heterogeneity	Connecting devices are used in the IoV in a variety of ways since they are deployed by various individuals, authorities, and entities. Furthermore, they have various resolutions, functionalities, and operating conditions. As a result, allowing the seamless presence of various devices at the same time is difficult. Combining such devices in a heterogeneous network, in particular, increases the degree of complexity.
2	Centralization	Smart vehicle architectures are currently focused on centralized, and mediated communication models. All of the vehicles are marked, authenticated, approved, and linked by central cloud servers. The malfunction of cloud servers will put the entire network at risk.
3	Lack of Privacy	In most current communication architectures, user privacy is not covered. In other words, data about the vehicle are shared without the consent of the owner.
4	Interoperability	In the IoV ecosystem, all human and non-human artifacts are treated as participants. In IoV applications, each actor may play a number of roles depending on the context and the situation, including service providers, data users, data providers, and available resources. It is important to ensure that all actors work seamlessly in order to realize the IoV vision.
5	Mobility	Protocol reliability and the IoT network are two problems for mobility. Due to substantial processor and energy constraints, sensor networks and mobile networks are currently not sufficiently configured to handle standard IoT applications.
6	Scalability	Because of the rapid development of embedded technology, the use of miniaturized devices (such as actuators and sensors) has increased. Simultaneously, the amount of data generated by these devices continues to increase indefinitely. As a result, another major IoV problem is managing the number of devices and the data they generate.

The limitations faced by authentication-based approaches are as follows: the AKM-IoV method in Reference 103 does not explore its application in a real-world deployment. Blockchain consensus technology was not considered in Reference 93 for identifying new vehicle authentication. Standard-enabled alternative mechanisms, like PANA, was not considered for obtaining trade-offs among features that were provided by various solutions.[107]

The research gaps of the trust-based approaches are explained as follows: the method in Reference 113 failed to consider other algorithms for finding the shortest path between an ordinary node and the controller node. The limitations of other blockchain-based techniques are as follows: in Reference 123, the considerable load overhead problem has occurred on both backhaul and radio layers, and it is also complicated for both deployment and management. The method in Reference 115 does not design application programming interfaces (APIs) among the blockchain network and SDN controllers based on REST API. The method in Reference 116 failed to solve the traffic issues of the specific vehicles.[116] Formal verification and formal modeling of BC was not considered in Reference 117. The pseudonym management system was not considered while implementing the BC concept in Reference 118. The adaptive consensus approach was not considered for BC-based IoV schemes.[120] In Reference 121, the contract theory was not considered to design an incentive mechanism for the V2G energy trading system.

The identified gaps and security challenges are tabulated as shown below in Table 9:

To address the existing gaps and limitations of the existing techniques, we propose 5G and IoV enabled blockchain technology to address the IoV security issues. One of the significant advantages of 5G is that it can overcome any issues between the physical devices and cloud server. A 5G-enabled Hyper speed network furnishes an incorporated disseminated accounting framework with consistent 5G connectivity for keen agreement framework, security framework, and a layered accord system. The 5G-enabled framework can address the issues of high-throughput and unpredictable, decentralized needs that are not addressed by the current solutions.

6 | CONCLUSION

This paper surveys different blockchain techniques to secure the IoV. The papers collected from the literature are classified based on their techniques, such as security, reputation, privacy, decentralization, data sharing, authentication, and trust-based approaches. The existing research work related to blockchain-based approaches to secure the IoV are analyzed, and their gaps with respect to the requirements are described. The following major gaps and research challenges were identified. (a) Lightweight design was not provided to improve the scalability issues. (b) Reinforcement and deep learning are not considered. (c) Adaptive consensus algorithms were not considered for improving the performance and scalability. (d) Incentive mechanisms could be designed to further improve the contract implementations. (e) With respect to the decentralized-based approaches, the existing methods are deficient in the abnormal network traffic monitoring. The gaps uncovered in this study can be studied further by the researchers to improve the field of blockchain-based IoV security work. Also based on our analysis in this study, we can conclude that the security-based technique is the most popular blockchain-based technique to secure the IoV compared to other techniques. Similarly, MATLAB is the widely used toolset to conduct research experiments to study the impact of blockchain-based techniques to secure the IoV. Among the performance evaluation metrics, cost, time, and utility are the popular metrics used for the experimental evaluation purposes. While we attempted to do as detailed a survey as possible in regard to the blockchain techniques for IoV security, and though we propose a 5G-based solution approach, this study is limited by the details of the proposed solution framework and architecture based on the existing gaps in the literature, and these issues will be handled in our future work.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Sarveshwaran Velliangiri https://orcid.org/0000-0001-9273-8181
Saru Kumari https://orcid.org/0000-0003-4929-5383
Sachin Kumar https://orcid.org/0000-0002-5324-2156

REFERENCES

1. Drljevic N, Aranda DA, Stantchev V. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Comput Stand Interf*. 2020;69:103409.
2. Yue L, Junqin H, Shengzhi Q, Ruijin W. Big data model of security sharing based on blockchain. Paper presented at: Proceedings of the 3rd International Conference on Big Data Computing and Communications (BIGCOM); Chengdu, China; August 2017.
3. Saha S, Chattaraj D, Bera B, Das AK. Consortium blockchain-enabled access control mechanism in edge computing based generic Internet of Things environment. *Trans Emerg Telecommun Technol*. 2020;e3995.
4. Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. Paper presented at: Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), November 2016.
5. Warkentin M, Orgeron C. Using the security triad to assess blockchain technology in public sector applications. *Int J Inform Manag*. 2020;102090:102090–102090.
6. Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: a blockchain based privacy preserving platform for healthcare data. Paper presented at: Proceedings of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage; 2017:534-543.
7. Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. Paper presented at: Proceedings of the NIST Workshop Blockchain Healthcare; vol. 1, 2016:1-10.
8. Mishra A, Gupta N, Gupta BB. Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. *Telecommun Syst*. 2021;77:1-16.
9. Mollah MB, Zhao J, Niyato D, et al. Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. *IEEE Internet Things J*. 2020;8(6):4157–4185.
10. Kumar S, Xu B. A machine learning based approach to detect malicious fast flux networks. Paper presented at: Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI); 2018:1676-1683; IEEE.
11. Eastman D, Kumar S. A simulation study to detect attacks on Internet of Things. Paper presented at: Proceedings of the 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech); 2017:645-650; IEEE.
12. Gohil M, Kumar S. Evaluation of classification algorithms for distributed denial of service attack detection. Paper presented at: Proceedings of the IEEE 3rd International Conference on Artificial Intelligence and Knowledge Engineering (AIKE); 2020:138-141.
13. Kumar S, Xu B. Vulnerability assessment for security in aviation cyber-physical systems. Paper presented at: Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud); 2017:145-150; IEEE.
14. Chelladhurai J, Chelliah P, Kumar S. Securing docker containers from denial of service (dos) attacks. Paper presented at: Proceedings of the 2016 IEEE International Conference on Services Computing (SCC); 2016:856-859; IEEE.
15. Kumar S, Bhargava B, Macêdo R, Mani G. Securing iot-based cyber-physical human systems against collaborative attacks. Paper presented at: Proceedings of the 2017 IEEE International Congress on Internet of Things (ICIOT); 2017:9-16; IEEE.

16. Chrane C, Kumar S. An examination of tor technology based anonymous internet. Paper presented at: Proceedings of the SITE 2015: Informing Science+ IT Education Conferences; 2015:145-153.
17. Kumar S, Vealey T, Srivastava H. Security in internet of things: challenges, solutions and future directions. Paper presented at: Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS); 2016:5772-5781; IEEE.
18. Srinivasan S, Alampalayam SP. Intrusion detection algorithm for MANET. *Int J Inf Secur Priv*. 2011;5(3):36-49.
19. Kumar S. Classification and review of security schemes in mobile computing. *Wirel Sens Netw*. 2010;2(06):419-440.
20. Alampalayam SP, Srinivasan S. Intrusion recovery framework for tactical mobile ad hoc networks. *Int J Comput Sci Netw Secur*. 2009;9(9):1-10.
21. Alampalayam S, Natsheh EF. Multivariate fuzzy analysis for mobile ad hoc network threat detection. *Int J Business Data Commun Netw*. 2008;4(3):1-30.
22. Alampalayam S, Kumar A, Srinivasan S. Mobile ad hoc network security-a taxonomy. Paper presented at: Proceedings of the 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005; Vol. 2, 2005:839-844; IEEE.
23. Alampalayam S, Kumar A. Predictive security model using data mining. Paper presented at: Proceedings of the IEEE Global Telecommunications Conference, 2004. GLOBECOM'04., vol. 4, 2004:2208-2212; IEEE.
24. Alampalayam S, Kumar A. An adaptive and predictive security model for mobile ad hoc networks. *Wirel Pers Commun*. 2004;29(3–4):263-281.
25. Alampalayam S, Kumar A. Security model for routing attacks in mobile ad hoc networks. Paper presented at: Proceedings of the 2003 IEEE 58th Vehicular Technology Conference, VTC 2003-Fall (IEEE Cat. No. 03CH37484); vol. 3, 2003:2122-2126; IEEE.
26. Alampalayam S, Kumar A, Srinivasan S. Mobile ad hoc network security-a taxonomy. Paper presented at: Proceedings of the 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005; vol. 2, 2005:839-844.
27. Kumar SA. Organizational control related to cloud. *Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments*. Hershey, PA: IGI Global; 2014:234-246.
28. Alampalayam S, Kumar A, Graham JH, Srinivasan S. Intruder identification and response framework for mobile ad hoc networks. *International Conference of Computers and Their Applications*; Honolulu, Hawaii: 2007:260-265.
29. Kumar S, Kumar A, Srinivasan S. Statistical based intrusion detection framework using six sigma technique. *IJCSNS*. 2007;7(10):333.
30. Samad A, Alam S, Mohammed S, Bhukhari MU. Internet of vehicles (IoV) requirements, attacks and countermeasures. Paper presented at: Proceedings of 12th INDIACom; INDIACom-2018; 5th International Conference on "Computing for Sustainable Global Development" IEEE Conference; 2018; New Delhi.
31. Alouache L, Nguyen N, Aliouat M, Chelouah R. Survey on IoV routing protocols: security and network architecture. *Int J Commun Syst*. 2019;32(2):e3849.
32. Garg T, Kagalwalla N, Churi P, Pawar A, Deshmukh S. A survey on security and privacy issues in IoV. *Int J Electr Comput Eng*. 2020;10(5):2088-8708.
33. Minitours L, Chalouf MA, Krief F. Survey on blockchain-based applications in internet of vehicles. *Comput Electr Eng*. 2020;84:106646.
34. Banerjee M, Lee J, Choo K-KR. A blockchain future for internet of things security: a position paper. *Digit Commun Netw*. 2018;4(3):149-160.
35. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J*. 2018;6(2):2188-2204.
36. Queiroz A, Oliveira E, Barbosa M, Dias K. A survey on blockchain and edge computing applied to the internet of vehicles; 2020. arXiv preprint arXiv:2011.13676.
37. Chaudhary R, Jindal A, Aujla GS, Aggarwal S, Kumar N, Choo K-KR. BEST: blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput Secu*. 2019;85:288-299.
38. Iqbal S, Haquey A, Zulkernine M. Towards a security architecture for protecting connected vehicles from malware. Paper presented at: Proceedings of the IEEE 89th Vehicular Technology Conference (VTC2019-Spring); 2019:1-5.
39. Li G, Wu J, Li J, Guan Z, Guo L. Fog computing-enabled secure demand response for internet of energy against collusion attacks using consensus and ACE. *IEEE Access*. 2018;6:11278-11288.
40. Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw*. 2018;32(3):78-83.
41. Kim MH, Park KS, Yu SJ, et al. A secure charging system for electric vehicles based on blockchain. *Sensors*. 2019;19(13):3028.
42. Qian Y, Jiang Y, Chen J, et al. Towards decentralized IoT security enhancement: a blockchain approach. *Comput Electr Eng*. 2018;72:266-273.
43. Singh M, Kim S. Introduce reward–based intelligent vehicles communication using blockchain. Paper presented at: Proceedings of the international SoC Design Conference (ISOCC); November 2019.
44. Ao L, Ogah C, Asuquo P, Cruickshank H, Zhili S. A secure key management scheme for heterogeneous secure vehicular communication systems. *ZTE Commun*. 2016;21:1.
45. Rowan S, Clear M, Gerla M, Huggard M, Goldrick CM. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels; 2017.
46. Huang X, Xu C, Wang P, Liu H. LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access*. 2018;6:13565-13574.
47. Rathee G, Sharma A, Iqbal R, Aloqaily M, Jaglan N, Kumar R. A blockchain framework for securing connected and autonomous vehicles. *Sensors*. 2019;19(14):3165.

48. Zhang XD, Li R, Cui B. A security architecture of VANET based on blockchain and mobile edge computing. Paper presented at: Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN); August 2018:258-259.
49. Xu Y, Wang G, Yang J, Ren J, Zhang Y, Zhang C. Towards secure network computing services for lightweight clients using blockchain. *Wirel Commun Mobile Comput*. 2018;2018:2051693, 12 pages.
50. Lapets A, NikolajVolgushev AB, Jansen F, Varia M. *Secure Multi-Party Computation for Analytics Deployed as a Lightweight Web Application*. Boston, MA: Computer Science Department, Boston University; 2016.
51. Bogdanov D, Laud P, Laur S, Pullonen P. From input private to universally composable secure multi-party computation primitives. Paper presented at: Proceedings of the 27th Computer Security Foundations Symposium; July 2014:184-198.
52. Micciancio D, Tessaro S. An equational approach to secure multi-party computation. Paper presented at: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science; January 2013:355-372.
53. Zhu R, Cassel D, Sabry A, Huang Y. NANOPI: extreme-scale actively-secure multi-party computationPaper presented at: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; 2018:862-879.
54. Rahman MA, Rashid MM, Barnes SJ, Abdullah SM. A blockchain-based secure internet of vehicles management framework. Paper presented at: Proceedings of the 2019 UK/ China Emerging Technologies (UCET); August 2019.
55. Kim SK. Enhanced IoV security network by using blockchain governance game; April 2019. arXiv preprint arXiv:, pp. 1904.11340.
56. Yin B, Wu Y, Hu T, Dong J, Jiang Z. An efficient collaboration and incentive mechanism for internet-of-vehicles (IoVs) with secured information exchange based on blockchains. *IEEE Internet Things J*. 2019;7(3):1582–1593.
57. Saied YB, Olivereau A, Zeghlache D, Laurent M. Lightweight collaborative key establishment scheme for the Internet of Things. *Comput Netw*. 2014;64:273-295.
58. Aroraa A, Yadavb SK. Block chain based security mechanism for internet of vehicles (IoV). Paper presented at: Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT); 2018.
59. Balasubramaniam Y, Sathyanarayanan PSV. Enhancing connected vehicle security with block chain; vol.4 August 2018.
60. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading in industrial Internet of Things. *IEEE Trans Indus Informat*. 2017;14(8):3690-3700.
61. Davi L, Hatebur D, Heisel M, Wirtz R. Combining safety and security in autonomous cars using blockchain technologiesPaper presented at: Proceedings of the International Conference on Computer Safety, Reliability, and Security; 2019:223-234; Springer, Cham.
62. Sharma V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). *IEEE Communi Lett*. 2018;23(2):246-249.
63. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Netw*. 2018;32(6):184-192.
64. Xu X, Xue Y, Qi L, et al. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Gener Comput Syst*. 2019;96:89-100.
65. Baza M, Nabil M, Lasla N, Fidan K. Blockchain-based firmware update scheme tailored for autonomous vehicles, Paper presented at: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC); 2019.
66. Liu K, Chen W, Zheng Z, Li Z, Liang W. A novel debt-credit mechanism for blockchain based data-trading in internet of vehicles. *IEEE Internet Things J*. 2019;6(5).9098–9111.
67. Asuquo P, Cruickshank H, Morley J, et al. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. *IEEE Internet Things J*. 2018;5(6):4778-4802.
68. Lei A, Cao Y, Bao S, et al. A blockchain based certificate revocation scheme for vehicular communication systems. *Future Gener Comput Syst*. 2019;110:892–903.
69. Jiang Q, Zhang N, Ni J, Ma J, Ma X, Choo K-KR. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Trans Veh Technol*. 2020;69(9):9390-9401.
70. Jiang Q, Ni J, Ma J, Yang L, Shen X. Integrated authentication and key agreement framework for vehicular cloud computing. *IEEE Netw*. 2018;32(3):28-35.
71. Khelifi H, Luo S, Nourz B, Mounglax H, Ahmed SH. Reputation-based Blockchain for secure NDN caching in vehicular networks. Paper presented at: Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN), 2018.
72. Kang J, Xiong Z, Niyato D, Ye D, In Kim D, Zhao J. Towards secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory. *IEEE Trans Veh Technol*. 2019;68(3):2906-2920.
73. Yang Z, Zheng K, Yang K, Leung VCM. A blockchain-based reputation system for data credibility assessment in vehicular networks. Paper presented at: Proceedings of the 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); October 2017:1-5.
74. Wang Y, Zhou S, Zhang N. BSIS: blockchain based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Trans Indus Informat*. 2019;15(6):3620-3631.
75. Liang H, Wu J, Mumtaz S, Li J, Lin X, Wen M. MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X. *IEEE Commun Mag*. 2019;57(10):77-83.
76. Park Y, Sur C, Kim H, Rhee KH. A reliable incentive scheme using Bitcoin on cooperative vehicular ad hoc networks. *IT Converg Pract*. 2017;5(4):34-41.
77. Dorri A, Steger M, Kanhere SS, Jurdak R. BlockChain: a distributed solution to automotive security and privacy. *IEEE Commun Mag*. 2017;55(12):119-125.

78. Stanciu A. Blockchain based distributed control system for edge computing. Paper presented at: Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS); 2017:667-671.
79. Jiang T, Fang H, Wang H. Blockchain-based internet of vehicles: distributed network architecture and performance analysis. *IEEE Internet Things J*. 2018;110:892–903.
80. Li J, Liu Z, Chen L, Chen P, Wu J. Blockchain-based security architecture for distributed cloud storage. Paper presented at: Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications and IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC); December 2017;408-411.
81. Sharma S, Ghanshala KK, Mohan S. Blockchain-based internet of vehicles (IoV): an efficient secure ad hoc vehicular networking architecture. *IEEE 2nd 5G World Forum (5GWF)*; Dresden, Germany: IEEE; 2019:452-457.
82. Saini A, Sharma S, Jain P, Sharma V, Khandelwal AK. A secure priority vehicle movement based on blockchain technology in connected vehicles. Paper presented at: Proceedings of the 12th International Conference on Security of Information and Networks; September 2019:1-8.
83. Liu Y, Wang K, Lin Y, Xu W. LightChain: a lightweight blockchain system for industrial internet of things. *IEEE Trans Ind Inform*. 2019;15(6):3571–3581.
84. Sharma PK, Moon SY, Park JH. Block-VN: a distributed blockchain based vehicular network architecture in smart city. *J Inform Process Syst*. 2017;13(1):3571–3581.
85. Ramaguru R, Sindhu M, Sethumadhavan M. Blockchain for the internet of vehicles. *Adv Comput Data Sci*. 2019;1045:412-423.
86. Sharma PK, Moon SY, Park JH. Block-VN: a distributed blockchain based vehicular network architecture in smart city. *J Inform Process Syst*. 2017;13(1):184–195.
87. Hassan A, Habiba U, Ghani U, Shoaib M. A secure message-passing framework for inter-vehicular communication using blockchain. *Int J Distrib Sens Netw*. 2019;15(2):1550147719829677.
88. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of trust: a decentralized blockchain-based authentication system for IoT. *Comput Secur*. 2018;78:126-142.
89. Angin P, BurakMert M, Mete O, Ramazanli A, Sarica1 K, Gungoren B. A blockchain-based decentralized security architecture for IoT. Paper presented at: Proceedings of the International Conference on Internet of Things; June 2018:3-18.
90. Yang Z, Yang K, Lei L, Zheng K, Leung VCM. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J*. 2018;6(2):1495-1505.
91. Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*. 2019;19(2):326.
92. Abubaker Z, Gurmani MU, Sultana T. Decentralized mechanism for hiring the smart autonomous vehicles using blockchain. Paper presented at: Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications; November 2019:733-746, Springer, Cham.
93. Liu Y, Yu FR, Li X, Ji H, Leung VCM. Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing. *IEEE Trans Veh Technol*. 2019;68(11):11169-11185.
94. Odiete O, Lomotey RK, Deters R. Using blockchain to support data and service management in IoV/IoT. Paper presented at: Proceedings of the International Conference on Security with Intelligent Computing and Big-data Services; 2017:344-362.
95. Skarmeta AF, Hernandez-Ramos JL, Moreno MV. A decentralized approach for security and privacy challenges in the internet of things. *IEEE World Forum on Internet of Things (WF-IoT)*; Seoul, Korea: IEEE; 2014:67-72.
96. Abdmeziem MR, Tandjaoui D, Romdhani I. A decentralized batch-based group key management protocol for mobile internet of things (DBGK). Paper presented at: Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; 2015:1109-1117.
97. Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J*. 2018;6(3):4660–4670.
98. Brousmiche KL, Durand A, Heno T, Poulain C, Dalmieres A, Hamida EB. Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchainPaper presented at: Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018:1281-1286.
99. Zhang L, Luo M, Li J, et al. Blockchain based secure data sharing system for Internet of vehicles: a position paper. *Veh Commun*. 2019;16:85-93.
100. Pouraghily A, Wolf T. A lightweight payment verification protocol for blockchain transactions on IoT devices. International Conference on Computing, Networking and Communications (ICNC): Internet Services and Applications; 2019:617-623.
101. Luong NC, Xiong Z, Wang P, Niyato D. Optimal auction for edge computing resource management in mobile blockchain networks: a deep learning approachPaper presented at: Proceedings of the IEEE International Conference on Communications ICC; 2018:1-6.
102. Mahmood Z, Ning H, Ghafoor A. A polynomial subset-based efficient multi-party key management system for lightweight device networks. *Sensors*. 2017;17(4):670.
103. Wazid M, Bagga P, Das AK, Shetty S, Rodrigues JJPC, Park YH. AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment. *IEEE Internet Things J*. 2019;6(5):8804-8817.
104. Wang X, Zeng P, Patterson N, Jiang F, Doss R. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE Access*. 2019;7:45061-45072.

105. Sharma R, Chakraborty S. BlockAPP: using blockchain for authentication and privacy preservation in IoV. Paper presented at: Proceedings of the IEEE Globecom Workshops; 2018:1-6.
106. Pal O, Alam B, Thakur V, Singh S. Key management for blockchain technology. *ICT Exp*. 2019;7(1):76–80.
107. Hernandez-Ramos JL, Pawlowski MP, Jara AJ, Skarmeta AF, Ladid L. Toward a lightweight authentication and authorization framework for smart objects. *IEEE J Selected Areas Commun*. 2015;33(4):690-702.
108. Li L, Liu J, Cheng L, et al. Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans Intell Transport Syst*. 2018;19(7):2204-2220.
109. Sharma R, Chakraborty S. BlockAPP: using blockchain for authentication and privacy preservation in IoV. Paper presented at: Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps); December 2018:1-6; IEEE
110. Zhang X, Wang D. Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain. *IEEE Access*. 2019;7:97281-97295.
111. Ferdous MS, Chowdhury MJM, Biswas K, Chowdhury N, Muthukkumarasamy V. Immutable autobiography of smart cars leveraging blockchain technology. *Knowl Eng Rev*. 2019;35:E3. In-Press.
112. Esposito C, Ficco M, Gupta BB. Blockchain-based authentication and authorization for smart city applications. *Inf Process Manag*. 2021;58(2):102468.
113. Arshad SU, Ahmed JS, Seemab B, Javaid N. A futuristic blockchain based vehicular network architecture and trust management system. Paper presented at: Proceedings of the 2019 International Conference on Advances in the Emerging Computing Technologies (AECT); 2020:1-6; Al Madinah Al Munawwarah, Saudi Arabia.
114. Fort M, Freiling F, Penso LD, Benenson Z, Kesdogan D. TrustedPals: secure multiparty computation implemented with smart cards. Paper presented at: Proceedings of the European Symposium on Research in Computer Security; September 2010; 34-48; Springer, Berlin, Heidelberg.
115. Mendiboure L, Chalouf MA, Krief F. Towards a blockchain-based SD-IoV for applications authentication and trust management. Paper presented at: Proceedings of the International Conference on Internet of Vehicles; 2018:265-277.
116. Sheas MT, Javaid N. Trust value: credit based decentralized trust management in vehicular network using blockchain technology. *Research Methodology in Information Technology (RMIT)*. New York, NY: Springer; 2019.
117. Gauhar A, Ahmad N, Cao Y, Asif M, Cruickshank H, Ali QE. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput Sec*. 2019;86:318-334.
118. Lei A, Cruickshank H, Cao Y, Asuquo P, AnyigorOgah CP, Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things J*. 2017;4(6):1832-1843.
119. Sharma V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). *IEEE Communi Lett*. 2018;23(2):246-249.
120. Liu M, Teng Y, Yu FR, Leung VCM, Song M. Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle. Paper presented at: Proceedings of the IEEE International Conference on Communications (ICC); 2019:1-6.
121. Zhou Z, Lu T, Xu G. Blockchain and edge computing based vehicle-to-grid energy trading in energy internet. Paper presented at: Proceedings of the 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2); 2018:1-5.
122. Salem M, Mohammed M, Rodan A. Security approach for in-vehicle networking using blockchain technology. Paper presented at: Proceedings of the International Conference on Emerging Internetworking, Data and Web Technologies; February 2019:504-515, Springer, Cham.
123. Wang K, Yin H, Quan W, Min G. Enabling collaborative edge computing for software defined vehicular networks. *IEEE Netw*. 2018;32(5):112-117.
124. Bickson D, Dolev D, Bezman G, Pinkas B. Peer-to-peer secure multi-party numerical computation. Paper presented at: Proceedings of the 2008 8th International Conference on Peer-to-Peer Computing; 2010:257-266.
125. Ames S, Hazay C, Ishai Y, Hazay C, Venkitasubramaniam M. Ligero: lightweight sublinear arguments without a trusted setup. Paper presented at: Proceedings of the SIGSAC Conference on Computer and Communications Security; October 2017:2087-2104.
126. Chang X, Yu Y-L, Yang Y, Xing EP. Semantic pooling for complex event analysis in untrimmed videos. *IEEE Trans Pattern Anal Mach Intell*. 2016;39(8):1617-1632.
127. Chang X, Ma Z, Yang Y, Zeng Z, Hauptmann AG. Bi-level semantic representation analysis for multimedia event detection. *IEEE Trans Cybernet*. 2016;47(5):1180-1197.
128. Luo M, Chang X, Nie L, Yang Y, Hauptmann AG, Zheng Q. An adaptive semi supervised feature analysis for video semantic recognition. *IEEE Trans Cybern*. 2017;48(2):648-660.
129. Wang H, Li Z, Yang L, Gupta BB, Choi C. Visual saliency guided complex image retrieval. *Pattern Recogn Lett*. 2020;130:64-72.

How to cite this article: Kumar S, Velliangiri S, Karthikeyan P, Kumari S, Kumar S, Khan MK. A survey on the blockchain techniques for the Internet of Vehicles security. *Trans Emerging Tel Tech*. 2021;e4317. https://doi.org/10.1002/ett.4317