International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

Vol. IV, No. 05, pp. 36-56, May

Privacy-Preserving Schemes in Blockchain Empowered Internet of Vehicles: A Survey

Shaik Mulla Almas[1], K. Kavitha[2]

[1]Research Scholar, Department of Computer Science & Engineering, Annamalai University, Annamalai Nagar, Chidambaram –608 002, Tamil Nadu, India.
[2]Associate Professor, Department of Computer Science& Engineering, Annamalai University Chidambaram–608002, Tamil Nadu, India.

***Corresponding author E-mail: mullaalmas27@gmail.com**

ABSTRACT: VANET is a mobile network of automobiles, roadside units, and other equipment that connects devices to improve road safety and traffic monitoring. Although this method benefits motorists, it has many security challenges that are vitalto traffic safety. It's crucial that only allowed cars send messages and denied vehicles never interfere. Thus, Blockchain, a promising technology used across many fields, has been investigated for use on the VANET system to encrypt information shared between wayside devices and automobiles. Distributed Ledger technology can assure data accessibility, correctness, and unlink ability in the Internet of Vehicles, but it cannot guarantee security. Thus, systems implementing this innovation should adopt secrecy techniques to address user privacy concerns. This research surveys the literature on Blockchain-based vehicular services and privacy solutions. The essential qualities and attributes of existing solutions are examined to provide a full and critical analysis of their contributions to the domain. It also directs researchers to Blockchain-licensed vehicle network system confidentiality investigations.

Index Terms: Block Chain; Distributed Ledger Technology; Vehicular Network; Privacy, Confidentiality

1. Introduction

On the Internet of Things (IoT) ecosystem, the internet of vehicles (IoV) has emerged as a model that characterizes intelligent autos. It falls under the umbrella of vehicle Ad-Hoc Networks, or VANETs for short. It increases both their scalability as well as their capabilities. Mobile Ad-Hoc Networks, also known as MANETs, are networks that connect mobile devices and transmit appropriate data in order to give only wayside applications such as safe driving, mapping, and accident avoidance. Among the communications that consumers may be unwilling to give, some examples include sensitive data like car tracking information, private information (such as vehicles id and existing address), and navigational data. In addition, it is anticipated that the frequency of autonomous transportation will considerably increase within a short period of time in the near future, making it necessary for VANET to manage new clues and personal data. Intruders and fraudulent users may also attempt to get personal details from a car in order to cause serious challenges for the road infrastructure and the protection of drivers. As a consequence of this, it is absolutely necessary to protect the privacy of the participants, ensure the safety of the personal information they are trading with one another, and prevent any detrimental attacks. In addition, making certain that the information that is transferred is not altered or used in an inappropriate manner by third parties. Hashing,

Merkle trees, and public-key cryptography are a few examples of the cryptosystems that can be used with blockchain technology, which is a decentralized technology that employs an irreversible digital ledger. Blockchain technology also ensures users' anonymity. Blockchain technology is therefore utilized to solve the problems described above.

2. VANETs

In the digital age, intelligent vehicles are essential for modern mobility. ITS has provided complete and innovative services to control difficult events and improve vehicular traffic management. Vehicular networks are ad hoc networks with vehicles as nodes. Vehicle communication uses wireless technologies [1].VANET, a MANET, supports V2V and V2I communication. VANET aims to improve vehicle occupant comfort and safety. VANET system design includes an On Board Unit (OBU), crub side Unit, Software Unit (SU), internet protocols, transmission domains, and internet. Each vehicle has an OBU that communicates with other vehicles and system infrastructure. Roadside RSUs are usually permanent. The user and OBU intersect graphically in the software unit. Mobile intranet access points, Road side Units, and a Wi-Fi access network for V2I communication make up the SU [2]. VANETs divide communication into two categories: DSRC, a fast radio communication protocol, governs vehicle-to-vehicle and vehicle-to-infrastructure communications. OBU and DSRC allow adjacent vehicles and Road Side Units to communicate with traffic units online [3].Table 1 describes Vanet's. As vehicles [7], in the VANET communication keep on entering and existing the highways require specific information about safety, like traffic congestion and road conditions to select a route for their destination. Timely delivery of information is very crucial, failing gives rise to delay in message reaching to the destination safely. L. Gafencu [8] stated that IEEE's Wireless Access in Vehicular Environments (WAVE) and ETSI's Intelligent Transport Systems (ITS) G5 lead vehicle communications security. These follow introductory schemes.

Table 1: *Description of essential Components of VANET*

S.No	Component	Description
1	Trusted Authority (TA)	A trustworthy, efficient third party tasked with registering other VANET modules. It could also communicate to the Roadside units securely over wired broadband. All vehicles and RSUs must be licensed with the TA before establishing the network. [4]
2	Roadside Unit(RSU)	It can supervise automobiles within its communication range and is used mostly on the roadside. RSUs that send a message between vehicles locally or to the TA can verify the message Integrity and legitimacy. [5]
3	On-Board unit(OBU)	The DSRC protocol enables automobiles equipped OBUs to interact with the other vehicles or RSUs. Each OBU does indeed have a tamper-proof device (TPD) to assure that no information is disclosed. [6]

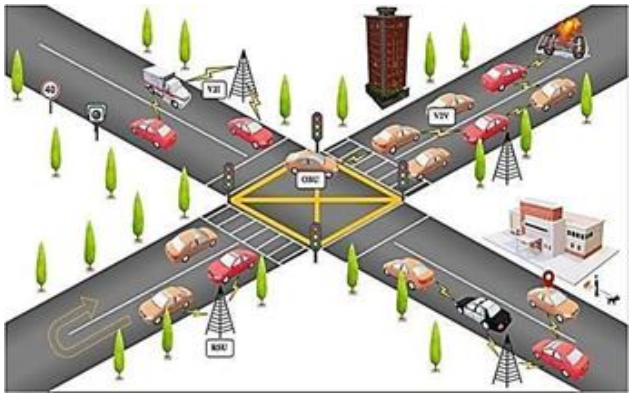


Figure 1: *Basic Infrastructure of Vehicular adhoc network Communication*

IEEE 1692 specifies message formatting, certificate handling, authenticating, signing, and revoking, while ITS G5 details architectonics, supervision, trust models, hazards, and overcoming network vulnerabilities with a central certificate authority. However, any new technology has hazards and threats. Bad data and fake attacks on data or network entities might cause disaster when cars are networked. Even though the IoV framework is good, it admits dangers. Attacks result from node mobility and intermediate engagement in the certification model. Real-time data attacks are faster due to bandwidth shortages. Many IoV attacks can upset drivers and the entire industry. This helps researchers consider integrity, confidentiality, and authentication more seriously. Depending on clutch location, dangers can be within or outside the clutch. One inter-clutch attack involves misleading vehicles to come over a desired zone to cause congestion, or self-driving vehicles can make wrong judgements based on mischievous data like road kidnapping [9]. This type of hostile vehicle must be detected to avoid affecting global data. Thus, cluster members must check attacker messages with regional registries to capture terrible vehicles. Vehicular and edge clouding can manage large amounts of data [10].One attacker can bypass authentication to utilize private credentials from approved nodes. IoV can undergo intra-cluster processing over time. The IoV subclass of IoT merges numerous technologies to generate a heterogeneous network. These technologies have their own principles and tactics. Any outside data from the enemy to environmental sensors can confuse the network.

Cloud hackers and other attackers can execute a DoS attack to disconnect legitimate users from the internet. Many scholars have researched the above assaults, which pose substantial threats to the Internet of Vehicles, to ensure its safety and anonymity. Security features are [11-14].See figure below: 2 illustrates Vanet security.

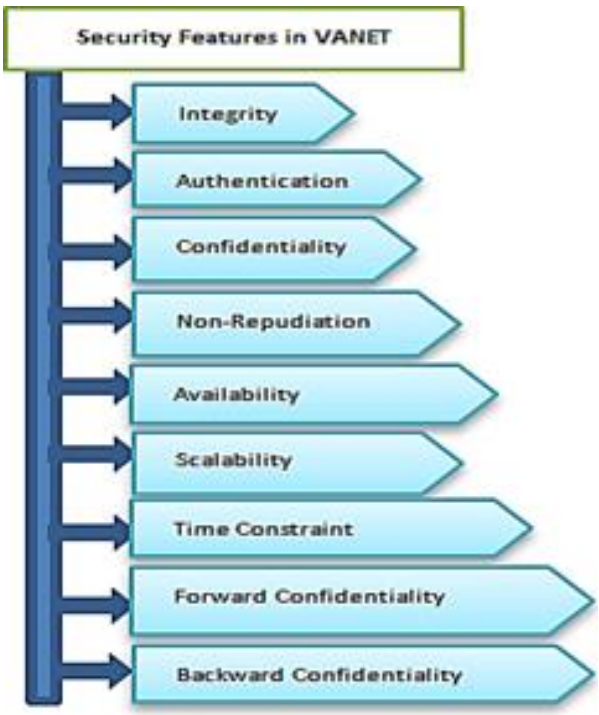


Figure 2: *Security Features in the IoV Environment*

Integrity: The content which is sent and received must be matching, where altering of the data should not take place in the network. Some of the possible attacks like tampering of messages, black hole attack, white hole attack, masquerading attack may take place.

Authentication: Forged vehicles should never be used to transmit information. The vehicles that receive the data should not be bluffed by the data of the fraudulent sender who lacks proper identification. The network is expected to distinguish among legitimate and unknown devices. The attacks on authentication are Sybil attack, which allow numerous participating nodes to join and make the network_s behaviour vulnerable to their attacks. A Black hole attack

delivers all data to the adversary, where the enemy drops the real time packets that help the drivers in making decisions regarding the safety. As a result of wormhole attack, the data will be routed to another channel with malicious users. A Fabrication attack permits a malicious to deliver faulty instructions that create distraction among the members of the region. Some other possible attacks on the Authentication are spoofing attack, sinkhole attack, malware, and masquerade and data modification assault.

Confidentiality: Although certain IoV information is intended to be accessible, the safety and confidentiality of IoV clientele is the critical component of the paradigm. As a result the confidential data should not be revealed to the adversary (Encryption must be applied).Analysis of the movement or content without even an adversary intruding into the channel is possible through Eavesdropping.

Non-Repudiation: In the event of road traffic accident, identifying the exact suspect is required. To do so all the users who are within the communication range of accident should not deny any message that is sent.

Availability: As when the number of vehicles on the road grows, the adherents of the IoV are increasing continuously leading to break down in the network due to congestion caused by requesting messages [12]. Some of the possible attacks on availability are Black hole attack, DoS attack, grey hole attack, advertising attack that sends phishing email all over the sunnet, consuming much bandwidth which affects the delay of the channel_s routine sessions, malware and jamming attack [9].

Scalability: The basis of exceptional dynamic topology depends on openness in rising network loads and nodes [11].

Time Constraint: Any delay in real time situations of IoV could be harmful. As a result, panic signals and warning should be delivered within time, without altering to implement exact results.

Forward Confidentiality: Internet of vehicles is as environment in which nodes mobility is dynamic leading to continuous change in the membership. As a result, it is the responsibility of the network to refresh the nodes all the time when it enters and exits the network, so that privacy can be preserved. Once the vehicle node exits the network it should not expose to the message of the internet.

Backward Confidentiality: When a replacement car node is included in system, it should not be notified with all the activities that have carried out before it's joining the network.

2.1 Classification Of Attackers: [1][2]

Rational attackers are straightforward to forecast, who perform attacks in the network for their own gain. The motive of the intruders is really to repair connectivity issues for selfish enrichment. Based on the behaviour in the network, attackers are classified [2].They are: (i) Internal versus External attacker (ii) Active versus Passive attacker (iii) Malicious versus Rational attackers.

Internal versus External Attacker: Internal attackers are the one who are authenticated and have accurate awareness about the Configuration of the network. Thus these attackers are very threatening and can propose complicated attacks than the other attackers. On the other hand the external attackers are less complicated than the internal attacker who is not authenticated.

Active versus passive attackers: Active attackers are the one who generate fake messages or who just don_t deliver them receive. Passive attackers get connected to Wi-Fi service in order to investigate the patterning on the speed of the information transmissions that are likely to be used for the upcoming.

Malicious versus Rational attackers: Some of the attacks are been sent by the threat actors to disturb the connectivity or cause problems for the intended victim.

2.2 Security Threats and attacks on VANETs: [1][2][4][15][16]

Impersonation Attack: This assault strikes authorized vehicles by broadcasting fraudulent notifications to certain other automobiles, where the attackers impersonate an authorized vehicle through using an authorized vehicle_s identity.

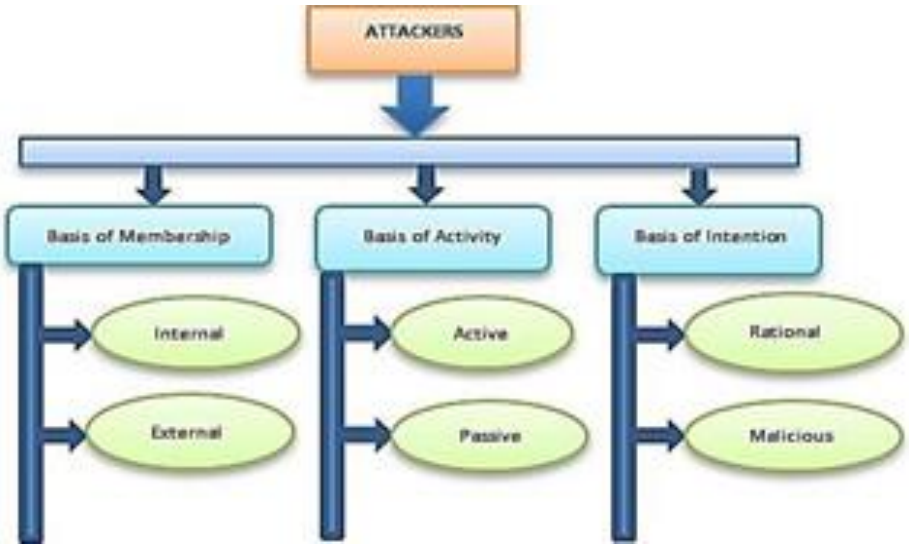


Figure 3: *Classification of attackers*

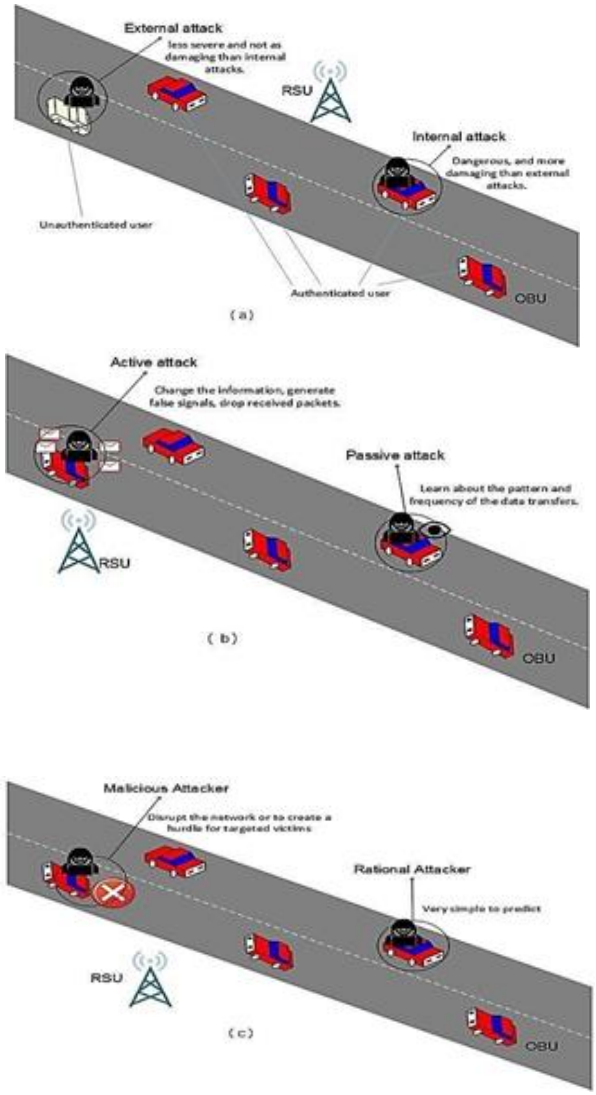


Figure 4: *Show the classification of attackers*

Modification Attack: Modified message will be transmitted into the network by the attacker to achieve definitive target. To attain a flawless path, attacker feeds false information to the vehicles which are nearby

Bogus Information Flow: Authenticated users get mislead by the attackers who circulate fraud information, where the authenticated users believe, accept the fictitious surroundings.

Message Poison Attack: In this attack, attackers gain control and authority over multiple nodes by passing authorized notifications, which are then utilised to transmit malevolent risk warnings.

Replay attack: In this assault, the adversary emphasize earlier circulated message in the network to lavishly exploit the channel_s resources and services.

Theft of cookies Attack: Just like a reply attack, the hacker preserves the credentials and leverages them to acquire network capacity as required in the future.[17]

Sybil attack: Attackers initiates some bogus vehicles all over the targeted vehicle that generates a jam signal, by which the targeted vehicle gets blocked.

Man-in-Middle Attack: Among the originator and recipient, the attacker get impersonated and receive most of the communications from the originator and forward them to the recipient in which the attack could be passive or active.

Denial-of-Service (DoS) Attack: The attacker launches a massive legitimate messages on to a particular communication channel of a network, where the network gets overloaded and capability of handling gets failed, as a result networks efficiency is reduced.

Masquerading Attack: This is identical to impersonation attack, where the attacker hijacks the listener by producing two distinct senders with the very same identification.

Warm hole attack: The adversary fakes its distance from the labelled node, causing communication from the transmitter flow over it, which causes dilemma and discloses all contents to the malicious node before flown into channel.

Eavesdropping Attack: During this invasion, these are passive attackers who gains confidential data transferred between two entities and illegally exploit them contrary to their privacy without their knowledge.

Message holding attack: These are the active attackers who dewdrop crucial messages about the road conditions, altering decisions of the drivers. These dropped messages will be saved by the drivers for the further usage in the network. [7]

Message manipulation attack: The attackers revise the messages so that it causes harm to the decisions taken by the receiving vehicle which disables the global system. Malware attack: This attack penetrates malignant bugs to taint the network in future. [17]

Session linking attack: This attack will be performed by linking random sessions like any automobile with several other communicating nodes, revealing credentials with some bit of calculation.

Fuzzy attack: Under this means of violence, the attackers communicate directly by cheating the identities by the stable data crawling of the system. In order to change the pattern of the identifier the attacker has to monitor the vehicle for quite a period of time. [18]

Data falsification attack: As a integrity attack, this attack creates bottlenecks and blocking with a minor modifications in the transmission. Author **[19]** proposed an algorithm which uses a contention window mechanism optimises the throughput. This is a spatial method which enables the headers of the network to interact with one another in order to lower capacity problems.

2.3 Security requirements in VANETS: [1][2]

Entity Authentication: A VANET communication recipient should be qualified to validate messages it has received and certify thesender_s legitimacy.

Message Authentication: Every communication received from RSUs and other vehicles must be authenticated by the vehicles, and the receiver must identify any alterations to the received messages.

Non-Repudiation: The transmitter just shouldn_t contradict the messages provenance when delivering it.

Low overhead: The elite security must be attained with minimum computational resources and least communication overheads between all the parties.

Traceability: As the vehicles in the VANETs are anonymous traceability is must and the only entity which is given privilege to perceive the identity of a vehicle is Trusted Authority (TA).Trusted Authority prevents malicious vehicles that try engage in the VANET Network.

Table2: *Attacks and threats in VANET and their counter measures.*

S.No	Attacks On	Types of attacks	Recommended remedies
1	Authentication	1. Sybil attack 2. Masquerading attack 3. Replay attack 4. Impersonation attack 5.Warm hole attack	1. Group signatures identity based. 2. Cryptography TamperedProof devices. 3. One time identity based aggregate signature. 4. Multiplicative secret sharing technique. 5.Individual message digital signature.
2	Availability	1. Channel interference attack 2. DoS attack	1. Hardware related side channels, Visual lights, ultrasonic audio. 2. Authentication method using Public Key Infrastructure (PKI). 3. Symmetric key cryptographic techniques.
3	Confidentiality	1. Eavesdroppi ng attack 2. Man-in-the – Middle attack 3.Message holding attack	1. Encryption
4	Integrity	1. Data Manipulation attack 2. Data falsification attack 3.Malware attack	1. Intrusion detection system 2.Packet message entropy

2.4 Privacy Requirements in the VANETs:

Preservation of Privacy: The vehicle, RSUs and third-party players shouldn_t fetch any information regarding the identity of the vehicles from of the received transmission.

Unlinkability: The RSU, car and following stakeholders shouldn_t even be able to trace behavior of the vehicles by examining the messages which were transmitted by the vehicles.

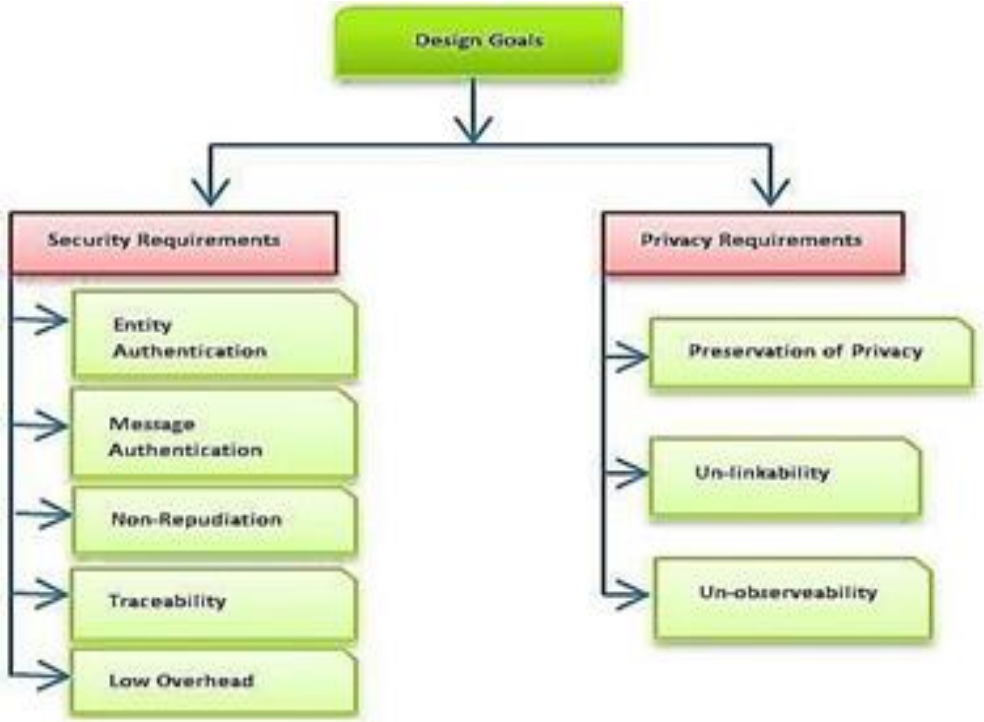


Figure 5: *Security and Privacy requirements for VANET*

Unobservaility: Observability is maintained during communication, where the broadcasting of the messages will be done by the vehicles without being perceived by others.

Entity Authentication: This is all about verifying the trustworthiness of the user_s.

Message Authentication: Verifying data consistency. Privacy Preservation: Never leaking the particulars about the node.

Non-repudiation: A sender after transmitting the message should not refuse message transmission.

Low Overhead: Bytes required for the communication and computational process should be low.

To protect security in VANET to cope with attacks, the security requirements that must be fulfilled are:

Table 3: *A comparison of available studies in the IoV*

S. No	Reference	Year	IoV Benefit	Security Requirement	Blockchain-based solutions for preserving privacy	Main points Included
1	B. Mokhta ret al [20]	2015	X	✓	X	1. Security threats and consideration s. 2. Categorizat ion of assault and vulnerabilities according to the OSI model multiple layers. 3. Talk about unanswered areas of research.
2	Sunil et al[2]	2015	X	✓	X	1. Security checks as well as the hazards they pose and the solutions they adopt. 2. Study initiatives in the long term.
3	J.Joy et al [10]	2017	X	✓	X	1. The advancement of Internet of vehicles from vehicles to cloud of the vehicles. 2. New IoV proposals.
4	M. A Talib et al[9]	2018	X	✓	X	1. Complete strategy to risks, assaults and their remedies is discussed. 2. Diverse solutions are shown.
5	R.Abassi [21]	2018	X	✓	X	1. Projects on Vanet. 2. Vanet Potential
6	J.Contrera s-Castillo [22]	2018	X	✓	X	1. The structure and Innovation of Vanets. 2. Security Criteria.
7	G.U. Devi[23]	2019	X	✓	X	1. Study on Internet of Vehicles (IoV), Internet of Things (IoT) & Internet of Everything (IoE). 2. New Research ideas were illustrated.
8	Our Survey	2022	✓	✓	✓	1. Study on attacks in Vanets, Blockchain based authenticati- on and privacy preserving schemes taxonomy is done.

3. Internet of Vehicles (IoV) in combination with Blockchain

Recording of transactions that are carried out among trust less peers is done in a distributed ledger called Blockchain [24]. This is an unalterable ledger that results in a chronological order of latest records called blocks, which consist of most newly arrived transactions. Blockchain postulated IoV is the most eye-catching technologies which provides solution to the latest centralized architecture [25]. Several basic applications of Blockchain that form Blockchain of Things [26]. Someof the advancing application as are as follows:1)Smart Grid [27][28] 2)Healthcare [29][30] 3)Smart Manufacturing [31] 4) IoT [32] 5)Industry 4.0 [33] 6)Smart transportation [34] and 7) Supply chain[35].

Blockchain is restricted to three leagues as Public, Private and Consortium Blockchain. Public Blockchain has an openness feature so that anybody can participate in, send, receive, and verify transactions. Some of the public Blockchain applications are crypto currency [36]. Ethereum, Private Blockchain is a completely authorized network, where the right to entry is only granted to a specific entity or a pool of entities.

Figure 6: *Designing Blockchain of Things Applications*

In this private Blockchain the master of the network makes a decision and allocates specific tasks to the remaining entities of the network. Consortium Blockchain is a hybrid of public and private Blockchain [37]. To work collaboratively across mentoring Blockchain nodes, there exists distinct consensus framework. Consensus procedures that are widely employed include: Proof-of-Work (PoW)‖, ―Proof-of-stake (PoS)‖, ―Byzantine faultTolerance (PBFT)‖.

The benefits of Blockchain implanted IoV is to brace immutability, decentralization, transparency and confidentiality also in smart grid systems also [38]. Authentication mechanism in collaboration with Blockchain for the security of data in IoV Environment is an anticipated research challenge [39].

3.1 Taxonomy of authentication and privacy schemes by Blockchain in IoV:

Authentication and privacy are the two major features which are necessary again for the creation of the trust in between vehicle inside a VANET [40]. Utilization of the apt identification and confidentiality system authentication and privacy schemes guarantee Vanet security and diagnose counterfeit nodes and bogus messages. Some of the authentication schemes is been proposed by many researchers to resolve frequent attacks on VANETs to safeguard secure communication.

Privacy in IoV: Privacy is the preparedness of a person or a group to safeguard the confidential information from illegitimate people [41].To preserve the privacy, there exists several technologies and methods [42].Particularly for IoV, it is pivotal to secure the privacy of users who are involved in the effective non-identical system comprising of countless participants who are not sure of each other. As vehicular services are growing, transferring of data also grows .Therefore preservation of privacy must be considered key feature during the design of the vehicular technology itself [43].The privacy of the members of IoV environment can be subdivided into following types:

Identity Privacy: Defending against the revealing of the users Identity using anonyms at the time of communication in VANET [44].

Location Privacy: Location of the user will be protected with the aid of overlaying/ clustering approaches.

Data Privacy: User_s personal data, much like speed, trajectory of the vehicles and the message transfers among the vehicles are been prevented from disclosure. By considering homomorphic encryption we can attain data privacy [45-47].

3.1.1 Related work:

From last few years so many survey are been made on privacy issues of Internet of Vehicles. The authors of [48] observed the existence of so many applications that are aiming to figure out and boost the security and privacy disputes of vehicular network. The authors of [49] revealed the security and privacy concerns of Internet of vehicles. Paper [50] expressed the interconnection between individual data and privacy in VANETS and also observed some of the existing proposals to solve the security and privacy matters during data exchange. In [51] authors concentrated on discussing about the solutions for privacy and security issues of 5G vehicular Network. The authors of the paper [52] focused on conventional security attacks. Also discussed regarding prevention of security attacks and protection against privacy in vehicular system.

Table 4: *Thinking map illustrates the classified scheme that emerged from the investigation of the papers included in this review.*

S. No	Privacy-Preserving solutions for Blockchain-enabled IoV			
1	Blockchain	Permissioned Blockchain	Hyper ledger Fabric	Practical Byzantine Fault, Tolerance, Proof Of Reputation, Proof Of Authority, Thermal Reactor.
		Permissionless Blockchain	Ether -eum	DAG, DPoS, Proof of Work, Proof of Location
2	Privacy Mechanisms	Pseudonyms	Tamper Proof Device ,Trust Authority , Certificate Authority , Public Keys, Service Provider	
		Homomorphic Encryption, Ring Signatures, CA- ABE Federating learning, Content Broadcasting, Blind Signatures, Group Signatures		
		Zero Knowledge Proof	ZKSNARKs, ZKRP, Parameters Comparison	
3	Service Areas	Authentication, Traffic Condition, Data Exchange, Dynamic Navigation, Reputation Management, General Services, Advertising		
4	Maturity	Proposal Simulation		
		Experimental	OMNet++, GoLang, PEPA, SUMO, OpenSSL, Truffle , Ropsten, NS-2, Matlab, VanetSim, Ropsten	

Several prevailing surveys have discussed about Authentication mechanisms in VANET.

In paper [53] the authors had made survey on authentication procedures that preserves the privacy of the vehicles. In [54] author discussed so many trust Models for VANET and focused on authentication setup that prevent privacy. The authors of the survey paper [55] concentrated on the privacy and security disputes that occur during data dissemination in VANET. In paper [56] the authors discussed about the location privacy prevention mechanisms in VANET.

In [57] authors shared content about location privacy and made a thorough review on trust models whose aim is to secure privacy and security in vehicular cloud computing. In [58], the authors scrutinised and evaluated present local differential privacy approaches and applications that support privacy presentation in Internet of Vehicles. In [59] authors made extensive survey on security with privacy features. This survey does not focus on privacy rather on other fields of Internet of Vehicles along with Blockchain Technology.

Some of the authentication procedure relating to Vehicular network are studied and evaluated [60]. Authors of this paper classified the mechanisms into cryptography, signature and verification and other privacy preserving features are been focused. The author of [61] discussed about the implementation of Blockchain technology together with Internet of Vehicles and analysed the solutions based on Blockchain technology for the Internet of Vehicles. They also explored different applications of VANET, where the Blockchain solutions are required and other open challenges are also discussed.

Even though lots of research are been carried out

regarding the privacy issues in the field of IoV, no much exposure is given on the Blockchain based solutions to this privacy disputes of IoV. Hence, in this work we tried to explore Blockchain-based solutions for preserving privacy of the entities in the network.

Table 5: *A Comparative studies on Security and Privacy Features*

Author Reference	Survey on Security and Privacy features	Identity Privacy	Location Privacy	Data Privacy
Luck et al[48]	✓	X	X	X
Garg et al[49]	✓	X	X	X
Akalu et al [50]	✓	X	X	✓
Bahtiyar et al [51]	✓	X	X	X
Kaiba et al [52]	✓	✓	X	X
Mathew etal [53]	X	✓	X	X
Lu et al[54]	X	✓	X	X
Maniva et al [55]	X	X	X	✓
Talat et al [56]	X	X	✓	X
Sheikh et al [57]	X	X	✓	X
Zhao et al [58]	✓	X	X	X
Mikavi et al [59]	✓	X	X	X
Azam et al [60]	✓	X	X	X

4. Blockchain Authentication

Several papers on Blockchain-based pseudonym management and authentication in automotive networks have been published, and they are listed below.

4.1 Authentication:

DAIA, a mechanism that ensures identity identification and privacy, was introduced by Liu et al. [62]. DAIA is a permissioned Blockchain that uses a tamper-proof gadget to generate a dynamic pseudonym. A Certification Authority (CA), vehicles, and Roadside Units (RSUs) are the major actors in this system. CA, like a base station, is now in charge of maintaining the chain of blocks as well as creating fresh blocks and also establishing security settings. Furthermore, it serves as a principal node recording all the information and broadcasting RSU_s publicly available information, as well as tracking rogue cars and maintaining a registry of them. It is claimed that it is also a reliable source that can trace the origins of a hazardous automobile. RSU_s have been stationed all around the roadway and therefore can control any car within its reach. The CA does have a wired network, while the vehicle has a wireless network. They can obtain the copy of the harmful car list from CA, which is regarded semi-trustworthy. The vehicles have a genuine tamper-proof device and an OBU.

The OBU is in-charge of wireless communication

systems, while the TPD is in-charge of storing and managing private variables, fake identities and passwords. TDP must often change the key due to attacks. This DAIA consist of five stages:

1. Registration: The controlled variables are issued by the CA.RSU chooses an SK_{rsu} at random and computes PK_{rsu}, the public key. RSU delivers CA its ID_{rsu} and PK_{rsu} identification codes. ID_{rsu} and PK_{rsu} are added to the Blockchain network by CA.TPD of a vehicle chooses private keys like SK_{TPD}, KID_v and a random parametera_n. Later CA receives an, KID_V and ID_V(true vehicular identification) from the vehicle.CA confirms that ID_V is valid (normally with the help of the national transportation Management Authority).CA generates a pseudo- PID_V, if the ID_V are legitimate.CA produces hashing chain hc with the help of a_n where h_c considered as a latest value. Certificate Authority starts writing PID_v, SK_s and h_c into TPD and saves h_c , KID_v and PID_V. Encryption of the vehicles confidential information and IDv_v is done through AES, with the key KID_V. Where Publish = Ek (ID_V, info) and the result of the encryption is published into the Blockchain network for the verification of the vehicles.

2. Pseudonymous Identity generation Phase: When the vehicle reaches specific RSU transmission distance, TDP evaluates the baseline parameters for the future communication .Using the PID_V which is issued by CA, the public key of the RSU (PK_{rsu}) and a_i of hash chain h_c in TPD, alias $SPID_v$ is computed for the time being. TPD therefore creates a momentary secret key SSK_v and calculates the public key SPK_v for it.

3. Communication phase: When the vehicle transmits a service request message to RSU, timestamp Ts is examined by RSU. If it is legitimate, then only RSU will accept the message and will broadcast it to the all other vehicles in the range.

4. Tracking Phase: When RSU wants to monitor a vehicle, it transmits a message called trace request message and the message sended by the vehicle to RSU to CA. Immediately CA performs some computation on data stored in its database and confirms that the vehicle can be traced and finally, CA adds the PID of the vehicle into the malicious vehicle registry and broadcasts the updated malicious vehicle list into the Blockchain platform.

5. Phase of parameters updating: When the network keys SK_s and PK_s exhaust, CA generates current format public keys PK'_s on the Blockchain network. Subsequently, CA encrypts new system private key SK'_s by symmetric encryption AES with the help of olden private key SK_s. The result $C_k = ESK_s (SK'_s)$ is delivered to Blockchain by Certificate Authority. TPDs will download C_k and PK'_s from the Blockchain platform and uses network private key SK_s for the decryption of C_k to retain SK'_s. RSUs will only download current system public keys PK'_s. As the Encryption key and Pseudonym PIDs lapses, latest will be generated by certain computations done by the vehicles TPDs.

4.1.1 Security Evalution:

This DAIA mechanism as a whole is designed to withstand the various malicious activities:

(i) Unlinkability: The vehicles genuine identification is recorded in the Certification Authority(CA) and TPDs, preventing an intruder from obtaining the keys. Furthermore, deducing it really is technically impractical. As a result, RSU is unable to derive relevant information regarding the entity.

(ii) Non-repudiation: Whenever an adversary attempts to modify temporary anonymity SPIDv, gets detected by RSU.As a consequence, the vehicle is unable to contradict that the communication was delivered by its own.

(iii) Secure Privacy Preservation: Even if an attacker controls all RSUs, the vehicles true identity remains hidden because RSUs solely possess SPIDv. The strict privacy objective has been accomplished.

(iv) Genuine TPD inference: The private

information in the TPD is constantly updated in our study, making it hard for the adversaries to acquire a large number of cipher messages using the same key.

(v) Man-in-the middle Attack protection: If adversaries try to modify any messages reaching RSU, it can be immediately detected by the RSU. This research primarily analyses the execution speed of six Vehicle -to-Infrastructure communication techniques like Zhou_s [63](Name of the authors considered as techniques), CPAS [64], EAAP [65], Tzeng_s [66] b –SPECS [67] and DAIA [62].ECC is used in Zhou_s authentication scheme. Batch-based evaluation on bilinear pairing is used to achieve verification in the CPAS and b-SPECS+ schemes. During verification phase asymmetric cryptography is used by EAAP. For message verification, Tzeng_s system employs batch-based ECC verification.

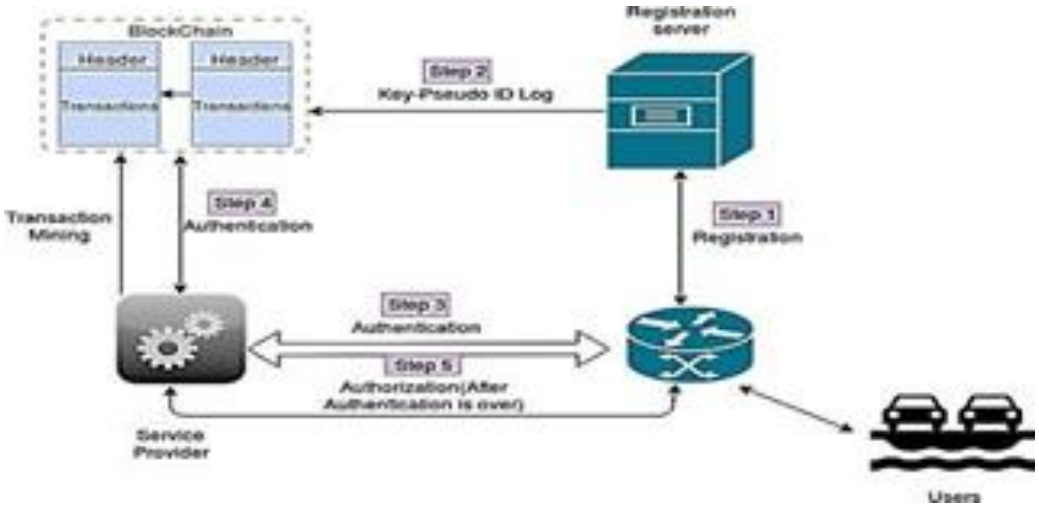
Some of the security features and denotations are: E1-Dynamic pseudonym, E2-Dynamic key,E3-Secure privacy preservation, E4-Restrictive tracking, E5-Non-repudiation. The suggested techniques is slower than others, but it offers greater security and robust privacy-preservation, making it perfect for realistic VANET contexts, according to security analysis and simulation.

Table 6: *Comparison of security features*

Security Features					
Schemes	**E1**	**E2**	**E3**	**E4**	**E5**
DAIA [62]	YES	YES	YES	YES	YES
Zhou‘s [63]	YES	NO	NO	NO	YES
CPAS [64]	NO	NO	YES	YES	YES
EAAP [65]	No	No	YES	YES	YES
Tzeng‘s[66]	YES	YES	NO	NO	YES
B-SPECS [67]	NO	NO	NO	NO	YES

In this work Sharma et al [68] presented a unique architecture for vehicular communication systems that uses Blockchain technology to assure the integrity of data, vehicle authenticity, privacy protection and smooth security systems across scattered service suppliers. A registration server, service providers, a Blockchain and vehicles are the four essential components of the proposed system. The registration server is usually in charge of monitoring and certifying vehicle identification numbers, which are later confirmed by service suppliers for vehicle authenticity. There is variety of service providers, each of which provides a variety of services to which a vehicle might subscribe. If approved vehicles can use numerous service providers simultaneously.

To gain access, a service provider and registration server must first register with a trustworthy central authority. Service providers are capable to read and write to the Blockchain, but the registration server will only be able to write to it. The Blockchain ensures that conflicts between multiple service providers over data and rights are resolved. The proposed system has three phases: The first is the registration phase, in which vehicles send and receive messages with the registration server to obtain a pseudo-id and be registered. The second phase is the authentication phase, in which service providers attempt to verify vehicles using pseudo-ids recorded in the Blockchain. Finally, the authentication step occurs, in which the vehicles submit service order messages to a service provider and the service provider adds the user_s access details with the approval status to the Blockchain as a collection of transactions.



During the registration phase, RSUs, vehicles and cloud platform act as intermediary access points to the registration server. During the authentication and authorization phase, they operate as intermediate network nodes to the service providers. There are two different types of blocks: one is placed by the registration server to keep records of registered vehicles and the other will be posted by service providers to keep count of access. In addition, there are three sorts of transactions: registration, authentication and authorization. The below Figure: **[69]** depicts the transaction template for each of the three transaction types

A transaction is only included in the block if it is found to be genuine; otherwise, it is discarded.

1. Registration phase: Vehicles are enrolled to the registration server with their original ids and are allocated pseudo ids and session keys for communication purposes with service providers during the registration phase.

Field Type				
Registration	Vehicle Pseudo id	Shared Secret	Session Details	Public Key
Authentication	Vehicle Pseudo id	Time- Stamp	Permission	Block-ID
Authorization	Vehicle Pseudo id	Access- Type(read /write)	Permission	Service-ID

Figure 8: *Transaction templates for each of the three transactions*

Pseudo id_s of vehicles being valid for a session, used for future communication that preserves vehicle privacy and avoids spoofing of ID_s .To get registered vehicles transmits a request message to registration server where the request text and vehicles original ID_s (may be vehicles registration number or driving license) are encrypted by public key of server. This original ID is supposed to be authenticated by trustworthy resources. The ECDH key exchange protocol is being used to exchange the keys. The public and private keys of a vehicle obtained during the key exchange are denoted as Pv and Pv_. After this key exchange, the registration server delivers the pseudo id to the vehicle and waits for the confirmation. Pseudo ID_s for vehicles are created by encrypting genuine ID_s with the registration server_s session public key.

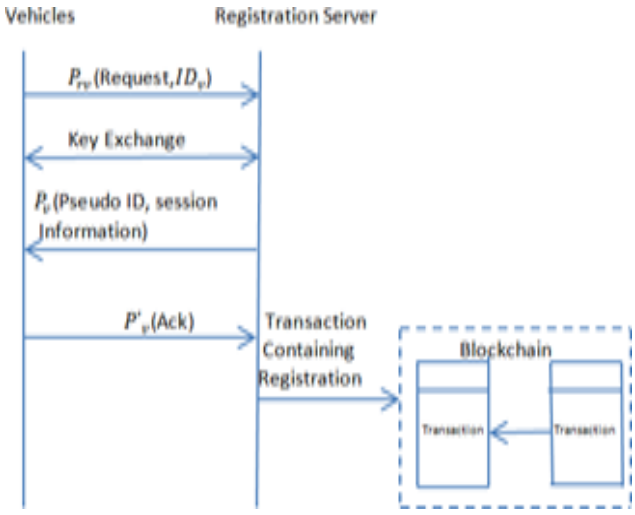


Figure 9: *Registration phase*

After the registration, the details of vehicles are delivered to Blockchain. If vehicles want any services they contact service providers. Vehicles pseudo-ID is transmitted in transparent form and access parameters acquired during registration are encrypted using vehicles private key.

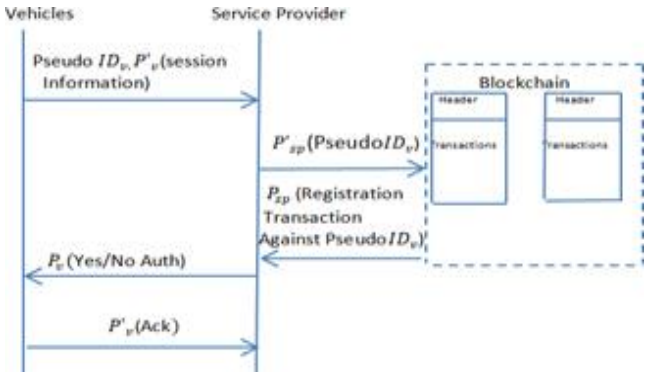


Figure10: *Authentication phase*

If the registration server wants to validate the transaction, it is delivered to each service providers; they store them in their local copy and awaits its addition to the Blockchain. Service provider certifies the transaction as genuine only after it is been published to the Blockchain. If the transaction is not added in to the Blockchain within session duration interval, the transaction is considered invalid. 3. Authorization phase: Every service provider keeps a public-private key pair one per service it offers, so that when vehicle subscribes for one, it gets the public key for that service. The vehicle transmits a service request message along with an electronic signature of the service under this phase. This will be encrypted by the vehicles private key. Once after checking this electronic signature and service ID, whether the digital signature belongs to the service providers, then only vehicle is permitted to read and write information about the service. Public key of a service is denoted by P_s. The connection will be halted when the service provider sends a termination message that will be confirmed from an acknowledgment from the vehicle. Once the digital signature is verified, the service provider uploads an authorization transaction to the Blockchain, which logs the vehicle_s authorization approval.

Authors created their system using the Ethereum Blockchain framework and smart contracts. Smart contract is a digital mechanism for implementing a coflict-free contract among several parties without the use of a third-party mediator.

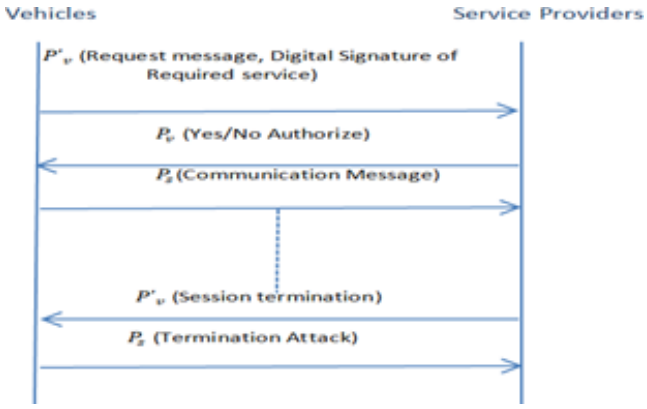


Figure 11: *Authorization Phase*

Ethereum exploits smart contracts built on top of Blockchain to allow developers to construct Blockchain-based apps. Smart contract is developed using solidity language and implemented using Remix platform. In this work, author presented a unique architecture for vehicle information systems that uses Blockchain Technology to guarantee data integrity, vehicle authenticity and privacy-preserving and smooth access control throughout decentralized service providers. This distributed Blockchain platform is useful for maintaining massive volumes of IoV data. By implementing the proposed regional caching technique, the issue of lengthy transaction times can be avoided.

5. Future Research Challenge and Issues:

IoV with physically secure Authentication:

A ―Physically Unclonable Function (PUF)‖ is indeed a one-way function that maps an array of issues to different sets of responses, dependent on the device_s unique physical microstructure [70].PUF is an important primitive for addressing many purposes such as authorization, security

systems and privacy. It can be used for low-cost and secure authentication [71].The essential characteristics of an optimal PUF are as follows [72]-[75]:

1. The PUF_s performance is always influenced by a physical world.

2. The PUF is simple to evaluate and construct.

3. The PUF_s output is unexpected and it functions as a random value.

4. Moreover, PUF cannot be cloned.

6. Conclusion

With its distinct properties, the IoV is a new technology and a possible research domain. Additionally, Blockchain is the best technology with IoV applications. However, it lacks built-in privacy protections, which are critical to the vehicular system. In this review study, we examined the literature on systems that have attempted to address many privacy challenges in IoV utilising Blockchain. As a result, we categorized, investigated and represented the privacy methods that were implemented, as well as the sectors where this methodology is being used. To tackle privacy issues, the offered categorization and evaluation of the proposed solutions indicate that indeed privacy- preserving approaches should be addressed and are already being investigated, in the Blockchain-enabled IoV environment. Pseudonymization seems to be the most extensively employed anonymity method in IoV, notably for enabling identity management in permissioned and permissionless architectures.

References

1. Mahmood A. Al-Shareeda; Mohammed Anbar; Iznan Husainy Hasbullah; Selvakumar Manickam, Year: 2020, “Survey of authentication and privacy schemes in vehicular ad hoc networks”, IEEE Sensors Journal, vol: 21, No: 2, pp: 2422–2433.
2. Sunil Kumar SManvi, Year: 2017, “Shrikant Tangade‖A survey on authentication schemes in VANETs for secured communication‖Vehicular Communications”, Vol: 9, pp: 19–30
3. Debiao He; Sherali Zeadally; Baowen Xu; Xinyi Huang, Year: 2015, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks”, IEEE Transactions on Information Forensics and Security, Vol: 10, No: 12, pp: 2681–2691.
4. Murtadha A. Alazzawi; Hongwei Lu; Ali A. Yassin; Kai Chen, Year: 2019, “Robust conditional privacy-preserving authentication based on pseudonym root with cuckoo filter in vehicular ad hoc networks”, KSII Transactions on Internet and Information Systems (TIIS), vol: 13, No: 12, pp: 6121–6144.
5. Murtadha A. Alazzawi; Hongwei Lu; Ali A. Yassin; Kai Chen, Year: 2019, “Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network”, IEEE Access, Vol: 7, pp: 71424-71435.
6. Yang Ming; Xiaoqin Shen, Year: 2018, “PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks”, Sensors, Vol: 18, No: 5, pp: 1573.
7. Omar Y. Al-Jarrah; Carsten Maple; Mehrdad Dianati: David Oxtoby; Alex Mouzakitis, Year: 2019, “Intrusion detection systems for intra-vehicle networks: A review”, IEEE Access, vol: 7, pp: 21266–21289.
8. Lucian Gafencu; Luminita Scripcariu, Year: 2018, “Security issues in the Internet of vehicles”, In 2018 International Conference on Communications (COMM), pp: 441–446, IEEE.
9. Manar Abu Talib; Sohail Abbas; Qassim Nasir; Mohamad Fouzi Mowakeh, Year: 2018, “Systematic literature review on Internet-of-Vehicles communication security”, International Journal of Distributed Sensor Networks, Vol: 14, No: 12, pp: 1550147718815054.
10. Joshua Joy; Vince Rabsatt; Mario Gerla, Year: 2018, “Internet of Vehicles: Enabling safe, secure, and private vehicular crowdsourcing”, Internet Technology Letters, Vol: 1, No: 1, pp: 16.

11. Yunchuan Sun; Lei Wu; Shizhong Wu; Shoupeng Li; Tao Zhang; Li Zhang; Junfeng Xu; Yongping Xiong, Year: 2015, “Security and Privacy in the Internet of Vehicles”, In 2015 international conference on identification, information, and knowledge in the internet of things (IIKI), pp: 116–121, IEEE.
12. Fengzhong Qu; Zhihui Wu; Fei-Yue Wang; Woong Cho, Year: 2015, “A security and privacy review of VANETs”, IEEE Transactions on Intelligent Transportation Systems, vol: 16, No: 6, pp: 2985–2996.
13. Ajay Kumar; Manu Bansal, Year: 2017, “A review on VANET security attacks and their countermeasure”, In 2017 4th international conference on signal processing, computing and control (ISPCC), pp: 580–585, IEEE.
14. Abdus Samad; Shadab Alam; S. Mohammed; M. Bhukhari, Year: 2018, “Internet of vehicles (IoV) requirements, attacks and countermeasures”, Proceedings of the 12th INDIACom, pp: 4037–4040.
15. Nishant Sharma; Naveen Chauhan; Narottam Chand, Year: 2018, “Security challenges in Internet of Vehicles (IoV) environment”, In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), pp: 203–207, IEEE.
16. Amit Dua; Neeraj Kumar; Ashok Kumar Das; Willy Susilo, Year: 2017, “Secure message communication protocol among vehicles in smart city”, IEEE Transactions on Vehicular Technology, Vol: 67, No: 5, pp: 4359–4373.
17. Abdulaziz Alshammari; Mohamed A. Zohdy; Debatosh Debnath; George Corser, Year: 2018, “Classification approach for intrusion detection in vehicle systems”, Wireless Engineering and Technology, Vol: 9, No: 4, pp: 79–94.
18. Danda B. Rawat; Moses Garuba; Lei Chen; Qing Yang, Year: 2017, “On the security of information dissemination in the Internet-of-Vehicles”, Tsinghua science and technology, Vol: 22, No: 4, pp: 437–445.
19. Bassem Mokhtar; Mohamed Azab, Year: 2015, “Survey on security issues in vehicular ad hoc networks”, Alexandria engineering journal, Vol: 54, No: 4, pp: 1115–1126.
20. Ryma Abassi, Year: 2019, “VANET security and forensics: Challenges and opportunities”, Wiley Interdisciplinary Reviews: Forensic Science, Vol: 1, No: 2, pp: e1324.
21. M. K. Priyan; G. Usha Devi, Year: 2019, “A survey on internet of vehicles: applications, technologies, challenges and opportunities”, International Journal of Advanced Intelligence Paradigms, Vol: 12, No: 1–2, pp: 98–119.
22. Salman A. Baset; Luc Desrosiers; Nitin Gaur; Petr Novotny; Anthony O'Dowd; Venkatraman Ramakrishna, Year: 2018, “Hands-on blockchain with Hyperledger: building decentralized applications with Hyperledger Fabric and composer”, Packt Publishing Ltd.
23. J. Hu; D. He; Q. Zhao; K.-K.-R. Choo, Year: 2019, “Parking management:A blockchain-based privacy-preserving system”, IEEE Consum. Electron. Mag, Vol: 8, No: 4, pp: 4549.
24. Hong-Ning Dai; Zibin Zheng; Yan Zhang, Year: 2019, “Blockchain for Internet of Things: A survey”, IEEE internet of things journal, Vol: 6, No: 5, pp: 8076–8094.
25. Chee-Wooi Ten; Koji Yamashita; Zhiyuan Yang; Athanasios V. Vasilakos; Andrew Ginter, Year: 2017, “Impact assessment of hypothesized cyberattacks on interconnected bulk power systems”, IEEE Transactions on Smart Grid, Vol: 9, No: 5, pp: 4405–4425.

26. Hongwei Zhang; Jinsong Wang; Yuemin Ding, Year: 2019, “Blockchain-based decentralized and secure keyless signature scheme for smart grid”, Energy, Vol: 180, pp: 955–967.
27. Lanxiang Chen; Wai-Kong Lee; Chin-Chen Chang; Kim-Kwang Raymond Choo; Nan Zhang, Year: 2019, “Blockchain based searchable encryption for electronic health record sharing”, Future generation computer systems, Vol: 95, pp: 420–429.
28. Thomas McGhin; Kim-Kwang Raymond Choo; Charles Zhechao Liu; Debiao He, Year: 2019, “Blockchain in healthcare applications: Research challenges and opportunities”, Journal of network and computer applications, Vol: 135, pp: 62–75.
29. Shubhani Aggarwal; Rajat Chaudhary; Gagangeet Singh Aujla; Neeraj Kumar; Kim-Kwang Raymond Choo; Albert Y. Zomaya, Year: 2019, “Blockchain for smart communities: Applications, challenges and opportunities”, Journal of Network and Computer Applications, Vol: 144, pp: 13–48.
30. Mandrita Banerjee; Junghee Lee; Kim-Kwang Raymond Choo, Year: 2018, “A blockchain future for internet of things security: a position paper”, Digital Communications and Networks, Vol: 4, No: 3, pp: 149–160.
31. Chao Lin; Debiao He; Xinyi Huang; Kim-Kwang Raymond Choo; Athanasios V. Vasilakos, Year: 2018, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0”, Journal of network and computer applications, Vol: 116, pp: 42–52.
32. Rajat Chaudhary; Anish Jindal; Gagangeet Singh Aujla; Shubhani Aggarwal; Neeraj Kumar; Kim-Kwang Raymond Choo, Year: 2019, “BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system”, Computers & Security, Vol: 85, pp: 288–299.
33. Srinivas Jangirala; Ashok Kumar Das; Athanasios V. Vasilakos, Year: 2019, “Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment”, IEEE Transactions on Industrial Informatics, Vol: 16, No: 11, pp: 7081–7093, doi: 10.1109/TII.2019.2942389.
34. Satoshi Nakamoto, Year: 2008, “Bitcoin: A peer-to-peer electronic cash system”.
35. ShaikMulla Almas; K. Kavitha; Y. Rajesh; B. Arun Kumar, Year: 2020, “Relative Investigation on Exploring Enterprise Blockchain of Kaleido, Azure Clouds and Deployment of smart Contract”, Vol: 13, No: 1.
36. Ahmed S. Musleh; Gang Yao; S. M. Muyeen, Year: 2019, “Blockchain applications in smart grid–review and frameworks”, IEEE Access, Vol: 7, pp: 86746–86757.
37. Muneeb Ul Hassan; Mubashir Husain Rehmani; Jinjun Chen, Year: 2019, “Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions”, Future Generation Computer Systems, Vol: 97, pp: 512–529.
38. Imran Makhdoom; Mehran Abolhasan; Haider Abbas; Wei Ni, Year: 2019, “Blockchain's adoption in IoT: The challenges, and a way forward”, Journal of Network and Computer Applications, Vol: 125, pp: 251–279.
39. C. Kalaiarasy; N. Sreenath; A. Amuthan, Year: 2019, “Location privacy preservation in VANET using mix zones–a survey”, In 2019 International Conference on Computer Communication and Informatics (ICCCI), pp: 1–5, IEEE.
40. Markus Christen; Bert Gordijn; Michele Loi, year: 2020, The ethics of cybersecurity, Springer Nature.
41. George Danezis; Josep Domingo-Ferrer; Marit

Hansen; Jaap-Henk Hoepman; Daniel Le Metayer; Rodica Tirtea; Stefan Schiffner, Year: 2015, "Privacy and data protection by design-from policy to engineering", arXiv preprint arXiv, pp: 1501.03726.

42. Hui Li; Lishuang Pei; Dan Liao; Gang Sun; Du Xu, Year: 2019, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET", Peer-to-Peer Networking and Applications, Vol: 12, No: 5, pp: 1178–1193.
43. Peng Hu; Yongli Wang; Bei Gong; Yongjian Wang; Yanchao Li; Ruxin Zhao; Hao Li; Bo Li, Year: 2020, "A secure and lightweight privacy-preserving data aggregation scheme for internet of vehicles", Peer-to-Peer Networking and Applications, Vol: 13, No: 3, pp: 1002–1013.
44. Gyanendra Prasad Joshi; Eswaran Perumal; K. Shankar; Usman Tariq; Tariq Ahmad; Atef Ibrahim, Year: 2020 "Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks", Electronics, Vol: 9, No: 9, pp: 1358.
45. Garg, T.; Kagalwalla, N.; Churi, P.; Pawar, A.; Deshmukh, S. A survey on security and privacy issues in IoV. Int. J. Electr. Comput.Eng. (IJECE) 2020, 10, 5409.
46. Aakash Luckshetty; Sindhu Dontal; Shrikant Tangade; Sunilkumar S. Manvi, Year: 2016, "A survey: comparative study of applications, attacks, security and privacy in VANETs", In 2016 International Conference on Communication and Signal Processing (ICCSP), pp: 1594–1598, IEEE.
47. Tanvi Garg; Navid Kagalwalla; Prathamesh Churi; Ambika Pawar; Sanjay Deshmukh, Year: 2020, "A survey on security and privacy issues in IoV", International Journal of Electrical & Computer Engineering , Vol: 10, No: 5, pp: 2088–8708 .
48. Akalu, Rajen, Year: 2018, "Privacy, consent and vehicular ad hoc networks (VANETs)", Computer law & security review, Vol: 34, No: 1, pp: 37–46.
49. Ezgi Tetik Sağlam; Şerif Bahtiyar, Year: 2019 "A survey: Security and privacy in 5G vehicular networks", In 2019 4th International Conference on Computer Science and Engineering (UBMK), pp: 108–112, IEEE. 2019.
50. Nazira Kaibalina; AE Mona Rizvi; Vol: 2018, "Security and privacy in VANETs", In 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), pp: 1–6, IEEE.
51. Deepu Mathew; Hima Anns Roy, Year: 2018, "A survey on different privacy-preserving authentication schemes in VANET", In IOP Conference Series: Materials Science and Engineering, Vol: 396, No: 1, pp: 012033, IOP Publishing.
52. Zhaojun Lu; Gang Qu; Zhenglin Liu, Year: 2018, "A survey on recent advances in vehicular network security, trust, and privacy", IEEE Transactions on Intelligent Transportation Systems, Vol: 20, No: 2, pp: 760–776.
53. Dakshnamoorthy Manivannan; Shafika Showkat Moni; Sherali Zeadally, Year: 2020, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)", Vehicular Communications, Vol: 25, pp: 100247
54. Hassan Talat; Tuaha Nomani; Mujahid Mohsin; Saira Sattar, year: 2019, "A survey on location privacy techniques deployed in vehicular networks", In 2019 16th International Bhurban conference on applied sciences and technology (IBCAST), pp: 604–613. IEEE.
55. Muhammad Sameer Sheikh; Jun Liang; Wensong Wang, Year: 2020, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey", Wireless Communications

and Mobile Computing 2020, No: 1, pp: 5129620.

56. Ping Zhao; Guanglin Zhang; Shaohua Wan; Gaoyang Liu; Tariq Umer, Year: 2020, "A survey of local differential privacy for securing internet of vehicles", The Journal of Supercomputing, Vol: 76, No: 11, pp: 8391–8412.
57. Branka Mikavica; Aleksandra Kostić-Ljubisavljević, Year: 2021, "Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey", The Journal of Supercomputing, Vol: 77, No: 9, pp: 9520–9575.
58. Farooque Azam; Sunil Kumar Yadav; Neeraj Priyadarshi; Sanjeevikumar Padmanaban; Ramesh C. Bansal, Year: 2021, "A comprehensive review of authentication schemes in vehicular ad-hoc network", IEEE access, vol: 9, pp: 31309–31321.
59. Leo Mendiboure; Mohamed Aymen Chalouf; Francine Krief, Year: 2020, "Survey on blockchain-based applications in internet of vehicles", Computers & Electrical Engineering, Vol: 84, pp: 106646.
60. Yi-Ning Liu; Song-Zhan Lv; Ming Xie; Zu-Bin Chen; Peng Wang, Year: 2019, "Dynamic anonymous identity authentication (DAIA) scheme for VANET", International Journal of Communication Systems, Vol: 32, No: 5, pp: 3892.
61. Yousheng Zhou; Siling Liu; Min Xiao; Shaojiang Deng; Xiaojun Wang, Year: 2018, "An efficient V2I authentication scheme for VANETs", Mobile Information Systems 2018, No: 1, pp: 4070283.
62. Lei Zhang; Qianhong Wu; Josep Domingo-Ferrer; Bo Qin; Chuanyan Hu, Year: 2016, "Distributed aggregate privacy-preserving authentication in VANETs", IEEE Transactions on Intelligent Transportation Systems, Vol: 18, No: 3, pp: 516–526.
63. Maria Azees; Pandi Vijayakumar; Lazarus Jegatha Deboarh, Year: 2017, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks", IEEE Transactions on Intelligent Transportation Systems, Vol: 18, No: 9, pp: 2467–2476.
64. Shiang-Feng Tzeng; Shi-Jinn Horng; Tianrui Li; Xian Wang; Po-Hsian Huang; Muhammad Khurram Khan, Year: 2015, "Enhancing security and privacy for identity-based batch verification scheme in VANETs", IEEE Transactions on Vehicular Technology, Vol: 66, No: 4, pp: 3235–3248.
65. Shi-Jinn Horng; Shiang-Feng Tzeng; Yi Pan; Pingzhi Fan; Xian Wang; Tianrui Li; Muhammad Khurram Khan, Year: 2013, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET", IEEE transactions on information forensics and security, Vol: 8, No: 11, pp: 1860–1875.
66. Rohit Sharma; Suchetana Chakraborty, Year: 2018, "BlockAPP: Using blockchain for authentication and privacy preservation in IoV", In 2018 IEEE Globecom Workshops (GC Wkshps), pp: 1– 6, IEEE.
67. Murtadha A. Alazzawi; Hongwei Lu; Ali A. Yassin; Kai Chen, Year: 2019, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network", IEEE Access, Vol: 7, pp: 71424–71435.
68. Satamraju, Krishna Prasad; B. Malarkodi, Year: 2020, "A PUF- based mutual authentication protocol for internet of things", 2020 5th International Conference on Computing, Communication and Security (ICCCS), IEEE.
69. Cédric Marchand; Lilian Bossuet; Ugo Mureddu; Nathalie Bochard; Abdelkarim Cherkaoui; Viktor Fischer, Year: 2017, "Implementation and

characterization of a physical unclonable function for IoT: a case study with the TERO-PUF", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol: 37, No: 1, pp: 97–109.

70. Prosanta Gope; Jemin Lee; Tony QS Quek, Year: 2018, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions", IEEE Transactions on Information Forensics and Security, Vol: 13, No: 11, pp: 2831–2843.
71. Alireza Esfahani; Georgios Mantas; Rainer Matischek; Firooz B. Saghezchi; Jonathan Rodriguez; Ani Bicaku, Silia Maksuti; Markus G. Tauber; Christoph Schmittner; Joaquim Bastos, Year: 2017, "A lightweight authentication mechanism for M2M communications in industrial IoT environment", IEEE Internet of Things Journal, Vol: 6, No: 1, pp: 288–296.
72. Nan Li; Dongxi Liu; Surya Nepal, Year: 2017, "Lightweight mutual authentication for IoT and its applications", IEEE Transactions on Sustainable Computing, Vol: 2, No: 4, pp: 359–370, doi: 10.1109/TSUSC.2017.2716953.
73. Francesco Marino; Corrado Moiso; Matteo Petracca, Year: 2019, "PKIoT: A public key infrastructure for the Internet of Things", Transactions on Emerging Telecommunications Technologies, Vol: 30, No: 10, pp: e3681, dio: https://doi.org/10.1002/spy2.97.