International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 5, October 2020, pp. 5409~5419
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i5.pp5409-5419

A survey on security and privacy issues in IoV

Tanvi Garg[1], Navid Kagalwalla[2], Prathamesh Churi[3], Ambika Pawar[4], Sanjay Deshmukh[5]
[1,2,3,5]Department of Computer Engineering, Mukesh Patel School of Technology Management and Engineering, NMIMS University, India
[3,4]Department of Computer Engineering, Symbiosis Institute of Technology, India

Article Info

Article history:

Received Dec 23, 2019
Revised Apr 17, 2020
Accepted Apr 28, 2020

Keywords:

Authentication
Internet of vehicles
Privacy
Security

ABSTRACT

As an up-and-coming branch of the Internet of things, internet of vehicles (IoV) is imagined to fill in as a fundamental information detecting and processing platform for astute transportation frameworks. Today, vehicles are progressively being associated with the Internet of Things which empower them to give pervasive access to data to drivers and travelers while moving. Be that as it may, as the quantity of associated vehicles continues expanding, new prerequisites, (for example, consistent, secure, vigorous, versatile data trade among vehicles, people, and side of the road frameworks) of vehicular systems are developing. Right now, the unique idea of vehicular specially appointed systems is being changed into another idea called the internet of vehicles (IoV). We talk about the issues faced in implementing a secure IoV architecture. We examine the various challenges in implementing security and privacy in IoV by reviewing past papers along with pointing out research gaps and possible future work and putting forth our on inferences relating to each paper.

Corresponding Author:

Tanvi Garg,
Department of Computer Engineering,
SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering,
Vile Parle, Mumbai, India.
Email: garg9925@gmail.com

1. INTRODUCTION

In today's day and age, transportation in many countries is being increasingly strained due to an increasing number of people. In many cases, the transportation system is obsolete, too costly to upgrade and changing it would prove to be too mammoth a task. An ongoing report noticed that the quantity of vehicles (traveller and business) utilized overall is somewhat higher than one billion [1] and is relied upon to arrive at two billion by 2035 [2]. The gigantic development in the number of vehicles causes an increment in vehicle blockage on streets, expanded fatalities and mishaps [3], and expanded contamination levels. Hence considerable changes in the transportation framework to adapt to rising prerequisites of new vehicles, travellers, and drivers is a purpose. With new ideal models, for example, the internet of things (IoT), distributed computing, and ongoing advances in figuring and systems administration advances have prompted the improvement of a wide scope of keen gadgets frequently furnished with implanted processors and remote correspondence advances. These savvy gadgets are being conveyed to give a protected and increasingly reasonable condition through their interconnection and interoperability, making another idea of IoT. Also, as rapid versatile Internet get to turns out to be progressively moderate and pervasive, physical boundaries, for example, separation becomes a non-substance and open doors for new items and administrations for society develop at a quicker rate, prompting better ways of life.

Few of these technological advancements have further led for the more complex but efficient branch in the department of transportation and that is the Internet of Vehicles. IoV requires software to tracks its movement and safeguard its network from malicious attacks. IoV exhibit self-driving, safety driving, social

driving, mobile applications and electric vehicles. The whole system co-ordinates and maintains communication between vehicle, roads, roadside units, sensors, humans all being the part of the network [4]. IoV synchronizes two high-tech dreams: 1) vehicle's networking and 2) vehicle's intelligence [5] and centres around the reconciliation of objects, for example, people, vehicles, things, systems, and situations to make an astute system dependent on computing and communication abilities that aids administrations, (for example, worldwide traffic productivity and the executives administration dependent on contamination levels, street conditions, clog traffic level, or vehicular security administrations) for enormous urban areas or even an entire nation.

By utilizing clever frameworks on vehicles and diverse digital physical frameworks, (for example, sensors, vehicles, and cell phones) in urban communities we can build up a worldwide system that offers various types of assistance to vehicles and the people related with them. IoV likewise alludes to vehicles, people, segments of the transportation framework, and a lot of gadgets apportioned in nature, associated through an all internet provider-based foundation, that trades data straightforwardly or by implication to contribute toward a progressively effective, more secure, and greener universe of transportation [6].

The fundamental contributions of this paper incorporate: first, a review of the various protocols, algorithms used by already published papers to help secure IoV along with the research gaps, future work and inferences of each paper; second analysis of various papers that can tackle most of the challenges present in the security and privacy of IoV by constructing an in-depth table; finally, we discuss our solution and inferences to accomplish a versatile, strong, secure, and completely operational IoV condition.

2. LITERATURE REVIEW

In [7], the author has stated that an autonomous vehicle unit (AUV) must have security requirements such as privacy, confidentiality, integrity, distributed denial of service (DDoS) protection and authentication. Attacks which disable the steering or brake system of a vehicle are more malicious on AUVs than on normal cars since there is no driver to use his/her intuition to minimize damage. Thus standards must be defined to protect AUVs from both internal and external attacks. Multifactor authentication factor can be one way to protect an AUV since it distinguishes between data reading and system control with priority given to system control. In this scheme, to obtain data to read requires only one credential factor but to access system control and vehicle onboard equipment requires authorization from multiple authorities. An AUV should also be able to prioritize activities and actions depending situations.

In [8], adaptive privacy is implemented wherein the privacy model is chosen by the user which helps to prevent data breaching and manipulation from unauthorized user. This paper discusses letting users choose their degree of privacy and find a balance between resource usage and privacy protocol. The proposed architecture is:

- The rationale for Adaptation: This works on the privacy requirements and reducing communication and computational overheads
- Anonymous authentication: this verifies whether the user is a valid member of the group and then every member is treated the same
- Probabilistic verification: in a common set the privacy degree and computational overhead is calculated with a probability method
- Group management: this method works on groups as users are characterised in groups therefore here the keys, information and grouping are taken care of.

In [9], the paper discusses various privacy and security attacks as well as the countermeasures required. It draws attention to authentication attacks which include Sybil attack, Masquerading attack, GPS deception, Wormhole attack; secrecy attacks, availability attacks, routing attacks and data authenticity attacks. The security requirements of a secure IoV architecture must include availability, high mobility of IoV entities, low errors tolerance, key distribution management and private routing of data.

The countermeasures to these attacks include:

- Threat modelling: Petri net modelling can be used in vehicular authentication, modelling and control of complex vehicular networks. Mathematical and Graph-based approaches can also be used to model network and integrity attacks.
- Intrusion detection system: protects against outside assaults by gathering and dissecting data from interior system frameworks to check if there exist infringement against the security approach.
- Honeypot: The system can include strategies to purposely engage and deceive hackers and identify malicious activities in the IoV architecture.

In [10], the paper talks about vehicular fog, which is like the Internet cloud for vehicles which provide services to autonomous cars. The common security requirements which must be present include confidentiality, integrity, privacy, and authentication. Physical attacks, like disabling a brake or steering

system pose grave threats in IoV. To avert mishaps, access to onboard units (OBUs) and CAN bus must be allowed using access control mechanisms. A simple password and id are not a secure means of allowing access to the OBUs. DoS attacks must also be taken into consideration while designing the vehicular network. Radio Frequency Jamming can also pose a threat since it can create large communication blind areas in which messages cannot be sent. This could lead to certain warning messages never reaching their intended target.

In [11], the paper discusses enemy endeavours to utilize data to build up the mapping connection among nom pseudonym virtual machine (VM) characters by coordinating a similar explicit area data, which raises genuine worries about area protection. The location-based service (LBS) suppliers get VM characters and continuous area data of vehicles from their LBS demands. The two information and protection spillage of outsider administrations and wellbeing messages incorporate area and personality-related data (e. For safe driving, vehicles intermittently communicate wellbeing messages {Pseudonym, Location, Velocity, Content, Time} to encompassing neighbours. The types of attacks on virtual machines include:

- Observation mapping attack: The arrangement is to supplant the VM personality by irregular identifiers and occasionally change the identifiers utilizing a VM identifiers replacement scheme (VIRS), which causes the mapping relationship to fall flat.
- Linkage mapping attack: A pseudonym changing synchronization scheme (PCSS) is proposed to protect against this assault. Right now, the procedure of pseudonym or alias and VM character substitution is synchronized to safeguard against linkage mapping assaults, which upgrades the security insurance level during driving.

In [12], the paper points out that for the safe route, forward impact warning, convergence crashes, traffic shockwaves, platooning and warnings about street hazards is an unquestionable requirement for V2V system. The security issue with V2I communication is that since it uses central navigators, all the information is uploaded on the navigator. The navigator stores critical information like the source, destination and speed of the vehicle.

The system generates personal data that is protected by aggregation servers such as electronic frontier foundation but there is a possibility that the aggregator colludes to compromise the privacy of the user and therefore, the paper utilizes the concept of haystack privacy. In haystack privacy, the vehicles with similar characteristics are grouped and only the common group characteristics are visible hence maintaining individual privacy. This is done when each data owner privatizes their data along with that a progression of Bernoulli trails randomizes the appropriate response and can frame a last totalled answer over the populace.

In [13], the paper examines the design, applications, and security, protection, and fairness of fog-based vehicular crowdsensing (FCVS). Manipulation of crowdsensing reports may directly impact the performance of an IoV architecture and further mislead users to make false decisions. Sensors on-board vehicles collect a lot of sensitive data such as PII and also the trajectory of a specific vehicle determined by using successive reports. Impersonation attacks and Sybil attacks may impact the IoV system by generating forged and false reports which could hamper other users. To achieve high-quality results in fog based networks, the tasks and location awareness property should be exposed but the identities of the vehicles performing these tasks must be protected. This is worth as far as protection since the cloud can't interface the characters of clients with the substance of undertakings, yet achieves the errands viably. A drawback is that pseudonyms need to be refreshed for each errand which is troublesome on the pseudonym administration for the two clients and the cloud, and group signatures are commonly computationally wasteful for clients. The paper proposes some sturdy security and protection insurance plans for vehicular crowdsensing applications, like:

- Secure tasking and reporting: Proxy re-encryption and searchable encryption along with a trusted third party should be involved in the key management.
- Privacy-preserving navigation: In [14], Ni et al. proposed a protection saving ongoing route framework to accomplish traffic-mindful route for drivers by using vehicular crowdsensing.
- Secure and DE duplicated crowd sensing: Information encryption gives a modern way to deal with forestall information spillage, then carrying a colossal deterrent to the intermediates for recognizing the reduplicated reports. To address these issues, Ni et al. [15] planned a haze based secure and deduplicated crowdsensing system. Right now, fog nodes are included to briefly store crowdsensing reports, and acknowledge proficient and make sure about information deduplication and commitment collection.

In [16], this paper discusses the several key security and scientific difficulties in haze helped vehicles. Aggressors can be portrayed as interior or outside and assaults can be dynamic or detached. An inactive assault doesn't wreck the usefulness of a vehicular fog registering framework however endeavours to unveil reserved information. A functioning assault is an endeavour to intentionally cut off

the activities of a vehicular haze registering framework (e.g., DDoS assaults, altering data of brilliant vehicles or the choice reports of fog nodes and cloud servers, and information exfiltration). The following properties should be implemented in vehicular fog computing:

- Confidentiality and Integrity: In vehicular fog computing integrity of data is crucial since tampering may result in disastrous consequences.
- Non-repudiation: No entity in the system can undo an action done previously such as the sending or receiving of information.
- Availability: Whenever an authorized vehicle attempts to access a fog node or cloud server, it is always ready for data retrieval or transfer.
- Relaibility and Forensics: Guarantees that the capacity to distinguish, gather, and examine the information from keen vehicles, haze hubs and the fundamental foundation for following and recognizing assailants continuously is working.

These previously mentioned prerequisites can be accomplished by utilizing cryptographic procedures. Homomorphic encryption can be utilized to accomplish mystery and usefulness.

In [17], the paper proposes a scheme which ensures location privacy-preservation with a report and data appropriation in IoV with the changed paillier cryptosystem, which empowers the roadside unit (RSU) to gather and convey the tactile information produced by vehicles. The paper suggests protection saving vehicular tactile information assortment conspire in IoV. The plan bolsters the RSU to play out the protection safeguarding composite information reports total and the outcome can be recovered and re-scrambled by the confided in rush hour gridlock the executives expert for additional preparing. The paper proposes a protection saving tangible information procurement conspire in IoV. The proposed plot empowers a vehicle to get the tactile information caught by different vehicles by safely questioning the information. The RSU re-encodes the accumulated tactile information into ciphertexts that must be completely recouped by the information questioning vehicle, while without the exposure of the information questioning area. There is a low data querying failure rate and the scheme is effective in terms of low computation cost and communication overhead. The paper states that the security requirements of the model proposed should include location privacy preservation, collusion resistance and data integrity.

In [18], the paper discusses security and privacy using the following:

- Authenticated crowd sourced data: The software controlling the vehicle is prone to malicious attacks misleading/forcing the vehicle to take a different/desired route. These spoofed messages should be detected and separated. This is secured by collecting the data and generating keys, sharing the data on authorized public platform and broadcasting data. The platform is authorized and every information is verified. This is so that all the information circulated is under the supervision and no such vehicles are misled.
- Scalable Privacy: Different methods like differential privacy work on protecting the privacy of the person giving them the option to control their flow of information. This trades accuracy for privacy but in the case to retain privacy accuracy is sacrificed. To not play with both, scalable privacy plays a part where the data is extracted from a big common group where only the common characteristics are displayed making it difficult to distort the owner's data.

In [19], the paper talks about the novel onboard units with three-level security architecture (NOTSA). There are different types of attacks that affect the CAN (controller area network) like:

- Short-range attack: attacker becomes a part of the network
- Long-range attack: attacker tracks the movement by attacking the navigation and radio function devices.
- DoS attack: The attacker sends a large amount of useless data into the system
- Eavesdropping attack: The attacker steals the private information about the victim and this information can help access other information on the network.
- Replay attack: Attacking the controller repeatedly hampers the normal functioning of the CAN
- Forgery attack: The attacker fakes to be a user device and controls all the commands

The NOTSA has four security areas with different functions:

- Area A: core security areas, this keeps in check all the users accessing data and authorising information exchange
- Area B: signal transmitting area, this has the transmitters that help area A take decisions, analyse devices in area C and make judgements in area D.
- Area C: consists of an external hardware device access area, keeps in check the external devices to prevent fraudulent acts on CAN.
- Area D: this is the external network access area, this controls all the traffic data and communication information amidst the vehicles.

To make NOTSA the secure architecture, it uses a three-level security precaution:

- Robust security verification and authentication to external networks and device: this says that all the external devices need to be authenticated and it is done with the algorithm as discussed in the paper
- Multiprocessor authentication: to authenticate these devices and networks an unclonable function is used that prepares an unpredictable response to challenges.
- Hardware isolation: this prevents the vehicles in the network from being controlled and also prevents weird malicious information from entering the network

To prevent different types of attacks on the network the security analysis says:

- That when the attacker disguises itself then the only way to differentiate between the legitimate and illegitimate users is when keys are decrypted to obtain the certificate and the difference is spotted saving the network.
- The unclonable function is also used so that the decision can't be predicted and henceforth the eavesdropping attack is avoided.

In [20], the paper discusses issues in the cognitive internet of vehicles (CIoV) are:

- Vulnerability Scanning for IoV: the CIOV does not have a device which can detect and act on vulnerabilities.
- Safe communication on interior network of IoV: this says that when CAN sends messages to the engine control unit (ECU), it cannot differentiate which node sends this message which may cause forgery and spoofing.
- Security on external network of IoV: interaction time should be lowered and difficult problems should be solved with a low-cost function.
- Integrity Protection and Security Upgrade for ECU Firmware: the trustworthiness and security should be guaranteed with some policy and authentication scheme.

In [21], the paper says that there three types of nodes, i.e. (i) cars, (ii) buses and (iii) pedestrians, that form social internet of vehicles (SIOV). These nodes are made keeping the common interests and are fully co-operated. In privacy-preserving interest-based forwarding scheme the community energy is of two types: Intra and Intercommunity energy. The privacy-preserving interest-based forwarding scheme for social internet of vehicles (PRIF) scheme include:

- System initialization: a trusted authority (TA) creates a group and generates a group ID. For any node to join these groups, the trust authority records it and produces an authentication in the form of a certificate. This is given to the node over a private authenticated channel.
- Privacy-preserving authentication: when a user claims to be associated with a particular group then his claim is validated by executing the privacy authentication.
- Forwarding process: when the vehicles are in the network, each node will communicate with each other various strategies are used to do this and maintain privacy.
- Message scheduling and buffer management: this uses the algorithms to manage efficient forwarding and authenticating the messages and buffers.

In [22], the paper reviews the benefits of IoVs, a proposed seven-layer architecture of IoV along with the protocols involved with IoVs. The security issue with IoV and preventing it from cyberattacks is critical. A security rupture could have extreme ramifications for drivers, travellers and different vehicles. The National Institute of Standards and Technology proposed a structure to improve cybersecurity and it ought to be followed for IoV also. The different security prerequisites are: Authentication, Integrity, Confidentiality, Data non-repudiation, access control, availability and anti-jamming.

In [23], this paper says, that the security model of pseudonym management has three layers, i.e. Cloud layer, fog layer and user layer. This architecture reduces overhead management, distributes pseudonym in a timely fashion. The proposed privacy-preservation pseudonym scheme also called at the P^3 scheme that the local authority generates and manages its pseudonym. This is done by:

- System initialization and key generation: initialize the vehicle, generate key and the pseudonym fog assigns the pseudonyms to the vehicles.
- Basic operation for pseudonym management: security messages along with a certificate, and time-stamp that notify the user to change its pseudonym.
- Local pseudonym requesting: before changing the pseudonym, the vehicle requests pseudonym for a new pseudonym.
- Context-aware pseudonym changing group: this depends on the number of vehicles so that the privacy is maintained and the tracking is difficult since many new pseudonyms are generated maintaining privacy by evaluating using a metric called pseudonym entropy.
- Local pseudonym changing: after the requesting change and verifying the stamped message, the vehicle changes its pseudonym

- Cross-region pseudonym requesting: when the vehicle is changing its region, it requests a pseudonym in the new region to get registered in the database of that region.
- Cross-region pseudonym changing: the new region receives the request, verifies it and changes the pseudonym

On evaluation, this paper maintains integrity and anonymity of the vehicle and fulfils the basic security requirements by taking care of various attacks. In [24], the paper reviews the ASC protocol and points out the problems plaguing the ASC protocol such as scalability problem, security problems like location spoofing attack, offline identity guessing attack, etc. The proposed protocol requires a user to register with a trusted authority. The trust authority picks a set of system parameters using one-way hash, which are prime field, generator field, a private and public key and a server secret. A user chooses a unique identity and sends it to the trust authority. The trust authority verifies the identity and subsequently, a smart card is issued. The smart card contains the system parameters and should be inserted into the vehicle. The user uses the smart card to connect to the trust authority at a nearby roadside unit to obtain a session key. The proposed protocol can provide mutual authentication based by contradiction. The paper describes various "games" which are simulations of the protocol. At the end of the games, it is proved that the advantage of the attacker is negligible.

In [25], the paper proposes a Security and Privacy-Based Access Control (SPBAC) model for the Web of associated vehicles. This model actualizes made sure about correspondence, totally unrelated consents relegated to clients sitting in the vehicles of a similar armada. It permits specialists to get to information and guarantees the use of dynamic separation of duty (DSD) inferable from conflicting consents. The security of armada is executed in layers which are separately overseen by various officials who are unconscious of movement in different layers. It portrays a bit by bit technique for checking access of a confirmed client.

Even though SPBAC is more secure than RBAC, DAC and MAC models, the limitations are that the childhood directories in DSD do not acquire tasks from various levelled parent indexes and duplicating and moving the registry is beyond the realm of imagination right now. In [26], the paper proposes a data collection approach based on a heterogeneous two-tier fog architecture for fog-based vehicle crowdsensing (FBVC) which aims to achieve privacy preservation, data aggregation, and traceability. The performance essentials that must be applied when designing crowd-sensing uploading and privacy protection mechanism are: Privacy preservation, data aggregation, secure communication, malicious vehicles. The proposed model has four layers which are:

- Sensing layer – Performs privacy protection and revocation.
- Lower tier Fog – Performs joint traceability.
- Upper-tier Fog – Performs secure query formation and carries out this secure query.
- Service Layer – Performs data support, data outsourcing and task assignment.

The Fog-based joint revocation mechanism involves the following steps: Initialization, Map list pre-treatment by fog buses, Invalid data identification, and Fog Based security search. In [27], the platooning control system is one of the various systems used to control autonomous vehicles. It involves a system that controls the lead vehicle's speed and direction. This data can be used by the third person that leads to data privacy and possibly service confidentiality failure. The privacy models discussed are:

- Differential privacy: This provides privacy when two databases differ by a single element.
- Distributional privacy: This allows privacy when databases differ in all of their elements.
- Crowd-blending privacy: This policy says take a random bunch of people and categorises based on common points so that when data is accessed only general characteristics turn up of the crowd and individual privacy is guaranteed.
- Random response model: as this paper suggests a Random Response model-based noise at the Encoder Shuffler trust limit to forestall vindictive shuffler. It recommends having an edge at shuffler analyser trust limit to turn away dangers and eavesdropping. Introduce noise at shuffler analyser interface to save it from the malicious analyser.
- ESA-extending privacy: this is a software that deals with encoding, shuffle and analyse. It encodes the records and shuffles them and analyse the incoming shuffled records based on the encrypted keys.

In [28], The Paper proposes an effective privacy-preserving validation conspire for energy internet-based vehicle-to-grid communication utilizing lightweight cryptographic natives, for example, single direction non-impact hash capacities. Right now, can safely get to administrations gave by a specialist organization utilizing the symmetric key set up between them. To guarantee dependable activity forestalling EI from cyberattacks is a need. The proposed plot depends on hash capacities and a three-party verification and key trade convention the proper investigation demonstrated that the plan is AKE-secure which is expected to accomplish protection from pantomime assaults or replay assaults, meeting key security and so

forth. Informal security analysis includes the following points: Protection against forgery attacks and Interception attacks, Privacy of the user, Protection against compromised user's device and Protection against physical attacks.

3. THREATS TO SECURE A PRIVATE NETWORK OF IOV

Discussed below are the main attacks and threats to the privacy mentioned in the papers, like the author [29], mentions about the various ways and the need to protect and monitor data sharing to preserve privacy. The papers mention the attacks dealt with attacks and the solutions to these attacks, that happen in various other fields like healthcare, various technological devices as addressed in [30-31], have also created a chaos in the IoV sector. These attacks as explained are:

- Sybil attack: It is an extreme attack on vehicular ad hoc networks (VANET) in which the attacker perniciously claims or takes different characters and utilize these personalities to upset the usefulness of the VANET arrange by dispersing bogus characters.
- Impersonation attack: malicious attackers may act like legitimate users and send reports to earn benefits and thus insert forged reports which can confuse and mislead customers. This is an impersonation attack.
- DoS and DDoS attacks: Denial-of-Service (DoS) assaults mean to make substantial exercises of a framework inaccessible. Because of a DoS assault, attackerss can't speak with one another, and vehicles don't get organize data, for example, street status, bringing about extreme outcomes. In a Distributed Denial-of-Service (DDoS) assault, nodes could dispatch an assault from various areas, in this manner making any discovery harder. Nodes propelling a DDoS assault could expect to hurt the vehicles in the system yet, in addition, RSUs, which are a significant part of the foundation in VANETs.
- Data non-repudiation: It is a legal idea that is broadly utilized in data security and alludes to assistance, which confirms the root of information and the trustworthiness of the information.
- Replay attacks: It exploits the conditions of the network by storing the messages to reuse it later when it becomes invalid and is not true.
- Forgery attacks: The attacker fakes to be a user device and controls all the commands
- Eavesdropping attack: also known as sniffing or snooping attack, happens when an unapproved party takes, alters or erases basic data that is transmitted between two electronic gadgets.
- Auxiliary attack: Where the attacker colludes to comprise the privacy by the aggregators
- Man in the Middle (MITM) Attacks: The man-in-the-middle idea is the place an aggressor or programmer captures a correspondence between two frameworks. It is a hazardous assault since it is one where the assailant acts like the first sender. As the assailant has the first correspondence, they can fool the beneficiary into speculation they are as yet getting a real message.

In Table 1, we address the different protection and security issues and draw a correlation that expresses all the issues happening in different papers. This encourages us to distinguish serious issues and thusly, causes us to chip away at them and infer a solution remembering these.

Table 1. Privacy and security issues addressed in previous literature

	[13]	[15]	[26]	[22]	[23]	[24]	[12]	[21]	[25]	[17]	[19]	[16]
Trusted Third-Party Validation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data encryption	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Sybil Attacks	✓							✓				
Impersonation Attacks	✓		✓	✓			✓	✓				
Privacy Techniques for vehicles	✓	✓	✓	✓	✓	✓		✓	✓		✓	
Privacy techniques for navigation	✓	✓	✓	✓	✓	✓		✓				
Fairness	✓	✓	✓	✓	✓	✓						
DoS Attacks			✓	✓						✓		
DDoS Attacks							✓					
Data non-repudiation	✓	✓	✓	✓	✓	✓						
Access Control	✓	✓	✓	✓	✓	✓						
Replay Attacks			✓	✓				✓		✓		
Forgery Attacks	✓		✓							✓		
Eavesdropping attack										✓		
Auxiliary attack							✓					
Collusion Resistance		✓	✓		✓	✓						
Data Integrity	✓	✓	✓	✓	✓	✓		✓	✓			
Man in the Middle Attacks			✓									
Session Key Security			✓							✓		✓

4. PROPOSED SOLUTIONS TO THE CHALLENGES OF SECURITY AND PRIVACY ISSUES IN IOV

As shown above, are some of the major problems that act as a barrier for a secure and safe network that also hinders with the privacy of its clients. To enhance the quality of the architecture and prevent mishaps due to attacks, there are a few solutions suggested below:

4.1. Authentication

This guarantees that any two correspondence units can verify the information in transmission. Sensitive data can be safeguarded using data encryption. However, data encryption triggers huge obstacles in terms of information sharing and searching since in IoV, shared data is used by other vehicles in the network to know the real-time information of traffic etc. Sources of data must be verified to make sure that untrusted or malicious reports do not reach customers since this may lead customers to make wrong decisions.

4.2. Access control

This intends to constrain fog node just to legal elements. This can be improved by using ECUs. Control can also be given to the trusted third party who authenticates the users before adding or giving out any information to the OBUs.

4.3. Confidentiality

Guarantees that any illicit endeavours to mess with information at- rest or data-in-transit in vehicular haze registering framework will be identified and forestalled.

4.4. Integrity

Guarantees that any illicit and unlawful endeavours to alter the data being transmitted or put away will be distinguished. In a vehicular fog computing framework, it is basic that the trustworthiness prerequisite is met since unsanctioned alteration may bring about genuine as well as deplorable outcomes, particularly in life-basic vehicular application settings, for example, a traffic control framework.

4.5. Non-repudiation

Guarantees that any article in the framework can't fix a past activity, for example, the sending or getting of information.

4.6. Availability

At whatever point, vehicular application endeavours to get to the fog nodes or cloud servers, they should consistently be prepared for transmission or recovery of information figure.

4.7. Reliability

Guarantees that all the data collected from fog nodes and smart vehicles are not fictitious or untrue. For this the routers should route the data to the required central system by looking at the location, preventing confusion of data. The data received should also be time-stamped and taken into consideration for only a particular amount of time after which the packet will discard and new information has to come in. The users sending this information has to be registered with the system. Trust is an important concept to accomplish security in the system, where each vehicle once furnished with a fitting trust model can assess the dependability of the got data and its sender [32].

4.8. Prevention against attacks

Several different kinds of malicious attacks can be tried against the data generated like impersonation attacks, forgery attacks, DOS attacks, Sybil attacks, etc. Often, malicious attackers may act like legitimate users and send reports to earn benefits and thus insert forged reports which can confuse and mislead customers. This is an impersonation attack. Attackers may likewise forge different personalities to convey unique or indistinguishable information to get more rewards or prevail in the factual choice procedure on reports. This is a Sybil assault. To oppose such assaults, boycott based verification ought to be manufactured, and productive discovery techniques on Sybil aggressors are required for the cloud. In DOS assaults, a server is blocked by loads of useless information and to prevent these attacks, there need to be authenticated users who can send and access information through the server, avoiding any random attacks. In forgery attacks, the attacker acts as a user device or the OBU sending out commands to control the network, to control this type of attacks, the original OBU should be protected with all steps of authentication and allow only verified users should be allowed to enter the network preventing any outsider getting access to any part of the system. An eavesdropping attack, the attacker accesses the location of

the user, driving information and to prevent this the concept of pseudonyms can be used since the name changes now and then the user won't be able to track the activities of the vehicle maintaining the individual privacy of the vehicle. Deployment of an unauthorized device can lead to false data injection which can severely hamper the performance of the network [33].

4.9. Privacy

Anonymity techniques like pseudonyms, group signatures, and k-anonymity can be used to protect vehicles' privacy. By using such techniques, vindictive aggressors are not able to separate vehicles dependent on swarm detecting information. In any case, it turns out to be difficult for the cloud to appropriate advantages to the comparing vehicles as per their particular commitments to undertakings once the group detecting reports are kept unknown. Whether or not swarm detecting information is conveyed namelessly, clients might need to discharge their group detecting errands without unveiling their characters. The assignments made open may contain some fragile data from which the aggressors can foresee the reasons why clients need to give these errands. Subsequently, how to designate the cloud to play out the group detecting assignments is fundamental for clients with the reasons for security protection and the nature of administration ensures. To get great outcomes, one exchange off is to uncover the undertakings, however, secure the personalities of the clients. This scarification is adequate for clients since the cloud can't interface the personalities of clients with the substance of assignments, however, achieves the errands successfully. Another technique for accomplishing security could be by actualizing outrageous focuses protection [34] which abuses the idea of the end focuses that are regular between vehicular social networks (VSNs) clients to make shared zones to anonymize them.

4.10. Trusted third-party involvement

A trusted third party is required to authenticate the users before adding them to the group and giving them the security key. Therefore, we need an unbiased third party to authorize every vehicle entering the network and activity that takes place preventing malicious attacks like impersonation attacks, forgery etc.

5. CONCLUSION

Framework in IoV stores a great deal of individual information like area, source position, goal, and so on and in this way keeping up security and protection is an exceptionally minor undertaking for them. An achievement in the field of IoV has prompted different research in the field, recommending various kinds of security and protection challenges in this field and their answers. There is a critical need to address this subject as a result of the progression in vehicles and everything being transferred on the web.

This paper examines the different issues that thwart the security and protection of IoV like DOS assaults, Replay assaults, Forgery assaults, an association of outsider and so forth. To beat these issues, it is examined that both the clients and the structures should be productive and contribute similarly to keep up the uniqueness of the client. We have proposed a couple of arrangements in this paper to manage the referenced assaults. The future extent of this paper will be a plan of a model that gives answers to these difficulties.

REFERENCES

[1] I. Wagner, "Number of Passenger Cars and Commercial Vehicles in Use Worldwide From 2006 to 2015 in (1,000 Units)," *Statista*, 2018.
[2] J. Voelcker, "It's Official: We Now Have One Billion Vehicles on the Planet," *Green Car Reports*, 2011.
[3] S. Al-Sultan, et al., "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380-392, Jan. 2014.
[4] M. N. O. Sadiku, et al., "Internet of Vehicles: an Introduction," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 1, pp. 11-13, Jan. 2018.
[5] Y. Fangchun, et al., "An overview of Internet of Vehicles," *China Communications*, vol. 11, no. 10, pp. 1-15, 2014.
[6] M. Nitti, et al., "On adding the social dimension to the Internet of Vehicles: Friendship and middleware," in *Proceedings of IEEE International Black Sea Conference on Communications and Networking*, Odessa, Ukraine, pp. 134-138, 2014.
[7] M. Gerla, et al., "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, pp. 241-246, 2014.
[8] K. Sha, et al., "Adaptive Privacy-Preserving Authentication in Vehicular Networks," *2006 First International Conference on Communications and Networking in China*, Beijing, pp. 1-8, 2006.
[9] Y. Sun, et al., "Security and Privacy in the Internet of Vehicles," *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Beijing, pp. 116-121, 2015.

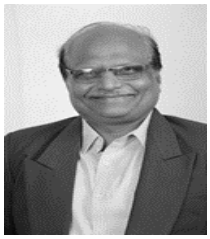
[10] E. K. Lee, et al., "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Fogs," *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, pp. 1-14, 2016.
[11] J. Kang, et al., "Location Privacy Attacks and Defenses in Cloud-Enabled Internet of Vehicles," in *IEEE Wireless Communications*, vol. 23, no. 5, pp. 52-59, Oct. 2016.
[12] J. Joy and M. Gerla, "Internet of Vehicles and Autonomous Connected Car - Privacy and Security Issues," *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, pp. 1-9, 2017.
[13] J. Ni, et al., "Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing," in *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146-152, Jun. 2017.
[14] J. Ni, et al., "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," *Proceedings of 2016 IEEE Vehicular Technology Conference (VTC-Fall)*, pp. 1-5, 2016.
[15] J. Ni, et al., "Secure and Deduplicated Spatial Crowdsourcing: A Fog-Based Approach," *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, 2016.
[16] C. Huang, et al., "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," in *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105-111, Nov. 2017.
[17] Q. Kong, et al., "A privacy-preserving sensory data sharing scheme in Internet of Vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644-655, Mar. 2019.
[18] J. Joy, et al., "Internet of Vehicles: Enabling safe, secure, and private vehicular Crowdsourcing," *Internet Technology Letters*, vol. 1, no. 1, pp. 1-6, 2017.
[19] L. Wang, et al., "NOTSA: Novel OBU with Three-Level Security Architecture for Internet of Vehicles," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3548-3558, Oct. 2018.
[20] Y. Qian, et al., "Secure Enforcement in Cognitive Internet of Vehicles," in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1242-1250, Apr. 2018.
[21] L. Zhu, et al., "PRIF: A Privacy-Preserving Interest-Based Forwarding Scheme for Social Internet of Vehicles," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2457-2466, Aug. 2018.
[22] J. C. Castillo, et al., "Internet of Vehicles: Architecture, Protocols, and Security," *Internet of Things Journal*, vol. 5, no. 5, pp. 3701-3709, Oct. 2018.
[23] J. Kang, et al., "Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627-2637, Aug. 2018.
[24] C. Chen, et al., "A Secure Authentication Protocol for Internet of Vehicles," in *IEEE Access*, vol. 7, pp. 12047-12057, 2019
[25] M. A. Habib, et al., "Security and privacy based access control model for internet of connected vehicles," *Future Generation Computer Systems*, vol. 97, pp. 687-696, Aug. 2019.
[26] G. Sun, et al., "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *Journal of Network and Computer Applications*, vol. 134, pp. 89-99, May 2019.
[27] M. Poddar, et al., "Privacy in the Internet of Vehicles: Models, Algorithms, and Applications," *2019 International Conference on Information Networking (ICOIN)*, Kuala Lumpur, Malaysia, pp. 78-83, 2019.
[28] P. Gope and B. Sikdar, "An Efficient Privacy-preserving Authentication Scheme for Energy Internet-based Vehicle-to-Grid Communication," in *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607-6618, Nov. 2019.
[29] Churi, Prathamesh P., and Ambika V. Pawar, "A Systematic Review on Privacy Preserving Data Publishing Techniques," *Journal of Engineering Science & Technology Review*, vol. 12, no. 6, pp. 17-25, 2019.
[30] Kagalwalla, N., Garg, T., Churi, P. and Pawar, A., "A Survey on implementing privacy in Healthcare: An Indian Perspective," *International Journal of Advanced Trends in Computer Science and Engineering* Available, vol. 8, no. 3, pp. 963-982, 2019.
[31] Kapoor, Vidhi, Rishabh Singh, Rishabh Reddy, and Prathamesh Churi, "Privacy Issues in Wearable Technology: An Intrinsic Review," *SSRN 3566918*, 2020.
[32] F. Ahmad, et al., "Trust Management in Vehicular Ad-Hoc Networks and Internet-of-Vehicles: Current Trends and Future Research Directions," *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities*, pp. 135-165, 2019.
[33] A.A.A. Ari, et al., "Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges," *Applied Computing and Informatics*, 2019.
[34] M. Babaghayou and A.A.A. Ari, "Location-Privacy Evaluation within the Extreme Points Privacy (EPP) Scheme for VANET Users," International Journal of Strategic Information Technology and Applications, vol. 10, no. 2, pp. 44-58, 2019.

BIOGRAPHIES OF AUTHORS

Ms. Tanvi Garg is a Computer Science undergraduate from SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India. Her area of interest includes security and privacy.

Mr. Navid Kagalwalla is a Computer Science undergraduate from SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India. His area of interest includes security and privacy.

Prof. Prathamesh Churi is PhD research Scholar in Computer Science and Information Technology Symbiosis International (Deemed University), Pune, India. He is also Assistant Professor of Computer Engineering Department from SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India. He is Associate Editor of International Journal of Advances in Intelligent Informatics (Indexed by Scopus), Indonesia. He has published more than 30 research papers in various international journals and conferences. He has been Co-Convener, Keynote Speaker, Session Chair and TPC Member of many reputed conferences at international level. His area of expertise includes Security and Privacy, Education Technology, Internet of Things.



Mr. Sanjay Deshmukh is a Ph. D. research scholar at AMITY university (Mumbai campus). He is currently employed as an Assistant Professor with Department of Computer Engineering for SVM's Mukesh Patel School of Technology, Management and Engineering, Mumbai, INDIA He has published several research papers in journals of repute. His interest area is artificial intelligence and Natural Language Processing.

Dr. Ambika Pawar is Associate Professor in Computer Science and Information Technology Department at Symbiosis International (Deemed University). She has more than 20 papers in the area of Cloud Computing, Data Privacy and Algorithms. She has experience of 10+ years in teaching as well as in research. She has been conference program committee member, Reviewer in various international conferences.