

# A Decentralized Authentication Model for Internet of Vehicles Using SSI

Victor Emanuel F. C. Borges<sup>1a</sup>, Danilo F. S. Santos<sup>1b</sup> and Dalton C. G. Valadares<sup>1c</sup>

*Future Connected Systems, Embedded Systems and Pervasive Computing Laboratory, Brazil*

**Keywords:** Internet of Vehicles, Vehicular Networks, Authentication, Self-Sovereign Identity.

**Abstract:** The Internet of Vehicles (IoV) ecosystem is well-regarded for its overall security, yet authentication remains a critical concern due to existing vulnerabilities that expose users to potential malicious attacks. Although researchers have devised authentication mechanisms and protocols to address these issues, there are two significant risk factors often overlooked by prevalent solutions. The first is trust in out-of-coverage mode, which can leave vehicles vulnerable to receiving forged messages. The second is the centralization of the standard authentication mechanism, where reliance on a centralized third-party service introduces authentication vulnerabilities that can result in access loss. In this article, we propose an innovative solution that incorporates the Self-Sovereign Identity (SSI) decentralized identity model within the Trust Over IP architecture to provide vehicular authentication. This integration establishes decentralized identification mechanisms suitable for various contexts within the IoV ecosystem. Our primary focus is enhancing security in the Advanced Driver-Assistance System (ADAS) context. We leverage the SSI model to design a specialized authentication scheme, aiming to effectively mitigate associated security risks through decentralization. This approach strengthens authentication security within the IoV ecosystem, addressing the mentioned vulnerabilities.

## 1 INTRODUCTION

In today's interconnected world, the Internet of Things (IoT) has permeated nearly every facet of our lives, from smart homes and wearable devices to industrial automation. One of the main areas of study in IoT environment today is the Internet of Vehicles (IoV). IoV represents a paradigm shift in the automotive industry, as vehicles become increasingly connected, intelligent, and capable of sharing critical information in real-time.


The major focus of the Internet of Vehicles field of study is on safety-related applications, which consider the physical safety aspects of the driver, passengers, pedestrians, and other entities involved. These scenarios include collision avoidance applications, post-collision notifications, lane change alerts, and blind spot alerts. However, this newfound connectivity also introduces a host of security challenges, with authentication standing as a paramount concern.


For securing data in these applications, their messages must be protected and encrypted, and they must not leak information about the user. Otherwise, it


would violate the privacy rights. Furthermore, it is essential to ensure that whoever sent the message is a genuine user and not a malicious one.

In summary, IoV needs to guarantee the authentication and anonymization of its involved entities, something challenging for a volatile and restricted technology such as the vehicular networks that implement the IoV ecosystem. To mitigate authentication-related threats, some researchers have proposed authentication mechanisms in various ways (Vasudev and Das, 2018) (Gayathri et al., 2018) (Islam et al., 2018) (Vijayakumar et al., 2017) (Cui et al., 2018). However, none of them solve critical cases related to the volatility of vehicles out of coverage and the decentralization of third-party entities. Therefore, considering a threat model based on these critical cases, this article presents a new authentication approach based on the Self-Sovereign Identity concept and the Trust Over IP architecture to mitigate these threats.

The remainder of this article is organized as follows. Section 2 overviews the current authentication issues and threats in IoV. Section 3 presents the state of the art of authentication mechanisms in IoV. Section 4 presents the considered threat model for this work. Section 5 introduces Self-Sovereign Identity model and Trust Over IP architecture for decentral-

<sup>a</sup>  <https://orcid.org/0000-0001-5346-8051>

<sup>b</sup>  <https://orcid.org/0000-0002-8162-715X>

<sup>c</sup>  <https://orcid.org/0000-0003-1709-0404>

ized authentication. Section 6 presents our proposed SSI-based vehicular authentication solution. Finally, Section 7 concludes this paper.

## 2 AUTHENTICATION ISSUES AND THREATS

In the context of IoV safety-related applications, most messages are transmitted via broadcast and need to be delivered in a short time. These messages must also be properly secured and encrypted to prevent data leakage.

To safeguard privacy, messages in the IoV system should never reveal their origin. Protecting the sender's identity ensures system anonymity. Additionally, for time-critical safety messages, the system must prioritize security without exceeding a 1200-byte limit, according to (3rd Generation Partnership Project, 2017).

Therefore, authentication mechanisms in the IoV ecosystem must be able to authenticate an entity to ensure that it really is who it claims to be, guarantee the anonymity of this entity, and ensure that the overhead of this entire process does not rise to the point of spending a significant amount of time and computational resources.

Common authentication mechanisms can be attacked through various techniques, such as network interference, eavesdropping, and intrusion. These attacks can compromise the IoV system, affecting the stability and robustness of the system or, in the worst case, crash the system and cause accidents.

One of the most significant vulnerabilities in an IoV system concerns user authenticity attacks, which occur through security gaps in the authentication mechanisms on the network. (Bagga et al., 2020) considers the most recent authentication mechanisms in the literature and categorizes them based on their algorithms into four types:

- *Sybil Attack*: The attacker creates some dummy vehicles around a target vehicle to generate a traffic jam signal while the path is clear enough, which forces the user to take a different route. This fake blocking is done using enumerable fake IDs for a single node, providing a gist of more than one node.
- *Wormhole or tunneling attack*: A malicious node fakes wrong information about its distance from the target node to make all messages coming from the sender flow through it. This creates a deadlock and exposes all messages to the attacker's node before flowing over a network.

- *Replay attack*: The adversary iterates over messages already transmitted within the network to reuse them and illegally access services and resources.
- *Masquerade attack*: The adversary uses the identity of some authenticated user, evacuating him from the network to mislead the innocent vehicles present and spoof them using false and dangerous messages. The adversary can spoof the receiver by creating two different senders with the same identity.
- *Message tampering*: An attacker modifies the content of messages to undermine the receiving entity's decisions by paralyzing the overall system.

In summary, two main factors enable authentication failures in IoV and open loopholes for security vulnerabilities and malicious attacks, which are listed below.

- In vehicular networks, nodes move swiftly and might enter out-of-coverage areas. In such cases without Trusted Authority, a vehicle trusts a message sender based on hardware compatibility, bypassing authentication. However, this can result in message tampering, where a fraudulent node sends fake messages to a real vehicle. Later, upon returning to coverage, the legitimate vehicle might relay this compromised data to applications (Twardokus and Rahbari, 2022).
- The reliance on a third-party service (Trusted Authority) for the system's centralized authentication mechanism, which verifies all entities, poses a risk to the IoV system. In case of a connection loss to a Road Side Unit (RSU) or Radio Access Network (RAN), authentication failure within the network can occur due to the centralized mechanism.

## 3 PROTOCOLS AND AUTHENTICATION MECHANISMS IN IoV

To address vehicular authentication challenges highlighted earlier, some authors have devised secure techniques, protocols, and authentication methods for IoV entities. They prioritize both security and minimizing the time and resource overhead in the authentication process.

(Bagga et al., 2020) considers the most recent authentication mechanisms in the literature and categorizes them based on their algorithms into five types:

Table 1: Notations of times required for unit operations in authentication.

Notation	Unit Operation	Time
Tecm	Elliptic curve point mult.	17.10 ms
Teca	Elliptic curve point add.	4.40 ms
Tmtp	Map-to-point operation	44.06 ms
Tbp	Bilinear pairing	42.11 ms
Th	One-way hash function	0.32 ms
Texp	Modular exponentiation	19.20 ms
Tenc/dec	Symmetric encr./decryption	0.32 ms

- *Lightweight Authentication:* These are the simplest and lightest authentication methods, ideal for the IoT context in general, but require auxiliary mechanisms for security. It guarantees security mainly against sybil attacks and replay attacks.
- *Batch Verification Based Authentication:* A batch verification method optimizes an authentication protocol by verifying the received signatures together in batches on the verifier side. Ensures security against masquerade attacks.
- *Privacy-preserving Authentication:* These are mechanisms that focus on preserving user privacy along with providing authentication. Ensures security against replay attacks and message tampering.
- *Dual Authentication:* These are methods that meet the demand for authentication by providing a dual authentication mode. It guarantees security mainly in sybil and message tampering attacks.
- *Hashchain-based Authentication:* Mechanisms that perform authentication based on a hash function, which are the ones with the least computational overhead. Mainly solves attacks related to data modification such as message tampering.

We examined the top-performing authentication mechanisms in each category, focusing on their time and computational efficiency (Bagga et al., 2020). We quantified time costs using unit operations and their approximate durations, as outlined in Table 1.

### 3.1 Lightweight Authentication

(Vasudev and Das, 2018) presented a two-tier lightweight authentication model featuring an upper layer housing a trusted vehicle server equipped with remarkable storage and computational resources, while the lower layer consists of vehicles. The protocol of this model encompasses a configuration phase, followed by registration and authentication phases that are seamlessly interconnected, ultimately enabling vehicle-to-vehicle (V2V) communication. No-

tably, this protocol brings forth advantageous outcomes such as reduced battery consumption, minimized communication overhead, lowered implementation costs, and improved processing time.

- Estimated time =  $4Th + 2Tenc/dec = 1.92$  ms
- Transfer of message size = 800 bits

### 3.2 Batch Verification Based Authentication

(Gayathri et al., 2018) introduced an authentication scheme based on batch verification, which offers a reduced computational overhead by eliminating the need for certificates and pairing techniques. This scheme ensures the security of authentication by addressing concerns related to tampering, traceability, anonymity, and revocation.

- Estimated time =  $5Th + 7Tecm + 3Teca = 134.5$  ms
- Transfer of message size =  $960n$  bits (where  $n$  is the batch scan of  $n$  messages)

### 3.3 Privacy-Preserving Authentication

(Islam et al., 2018) present a conditional privacy-preserving authentication protocol and group key generation protocol based on passwords, designed to minimize memory usage by the Trusted Authority. This scheme ensures identity maintenance and provides authentication, forward and reverse secrecy. Moreover, it offers robust security against replay, impersonation, modification, and offline password guessing attacks.

- Estimated time =  $10Th = 3.2$  ms
- Transfer of message size = 1632 bits

### 3.4 Dual Authentication

(Vijayakumar et al., 2017) propose a scheme that incorporates double authentication to prevent the entry of malicious nodes into the network. After authentication, the TA message is multicast to all authenticated vehicles. The message multicasting process utilizes a key calculated through the utilization of the Chinese Remainder Theorem (CRT). This scheme ensures security against various attacks, including Sybil attacks, spoofing, replaying, fabrication, altering message moderation, and collusion attacks. Additionally, the proposal maintains secrecy in both directions, ensuring confidentiality of communication.

- Estimated time =  $2Th + 4Texp + 6Tenc/dec = 79.36$  ms

- Transfer of message size = 3168 bits

### 3.5 Hashchain-Based Authentication

(Cui et al., 2018) introduce a hashchain-based proposal for conditional privacy protection, leveraging the use of a hash function. While many protocols rely on bilinear pairing or elliptic curves, this protocol stands out as the most cost-effective option by employing simple hash functions. The scheme excels in privacy preservation, detection of malicious nodes, ensuring message authenticity and integrity, maintaining secrecy, and offering protection against replay, impersonation, and modification attacks.

- Estimated time =  $5Th = 1.6$  ms
- Transfer of message size = 1312 bits

### 3.6 Summary of the Solutions

Of the studied solutions, the strategy of (Cui et al., 2018) is the most efficient in terms of security against malicious attacks and preservation of privacy, at the same time that it does not increase the overhead considerably, nor does it need auxiliary security mechanisms as in lightweight category protocols.

However, none of the mechanisms studied can solve the fact that authentication in the IoV ecosystem is centralized and dependent on a third-party service in a Trusted Authority. In fact, this is an open research question according to some studies (Bagga et al., 2020) (Alladi et al., 2020) (Xi et al., 2022).

One of the potential solutions cited in the literature is the creation of a blockchain-based authentication mechanism, one of the prominent technologies that can provide the solution for today's centralized infrastructures. The advantages of using the blockchain-based IoV system is to support decentralization, immutability, transparency, confidentiality and trust, such as smart grid systems (Musleh et al., 2019).

Considering this gap in current authentication mechanisms, we've crafted a threat model to analyze how a malicious entity might exploit out-of-coverage vehicles and disrupt both centralized and third-party authentication systems.

## 4 THREAT MODEL

Our threat model use the Cellular-V2X communication standard, proposed by 3GPP (3rd Generation Partnership Project, 2017), which uses PC5 interface for vehicle-to-vehicle (V2V) communication, and Uu

interface for vehicle-to-network (V2N) communication. In the proposed scenario, we wish to investigate potential authentication threats related to the Advanced Driver-Assistance System (ADAS) application, widely used in IoV ecosystem.

The threat model can be seen in Figure 1 and follows the steps below:

- When vehicles are out of coverage, that is, without access to cellular network, they automatically switch to using out-of-coverage communication mode. The trust in this interface is established via hardware (meaning having a compatible OBU is sufficient).
- If we introduce a fake node that possesses a compatible OBU, it will be capable of transmitting false messages to a neighboring OBU through vehicle-to-vehicle communication (V2V). The affected OBU must, at some point, regain coverage and be reallocated to in-coverage communication mode.
- The affected OBU will transmit manipulated information to the eNb RAN through vehicle-to-network communication (V2N).
- The ADAS application server will capture this data and might make incorrect decisions based on it, subsequently transmitting them to the eNb RAN.
- The eNb RAN will broadcast data with erroneous decisions to neighboring OBUs via V2N.

Considering the proposed threat model, in the next section we will present a framework that can be used to develop a decentralized authentication solution plan to address this issue.

## 5 SSI-BASED AUTHENTICATION & TRUST OVER IP IDENTITY ARCHITECTURE

Self Sovereign Identity (SSI) is a model of decentralized identity that promotes the control and individual ownership to entities of their digital identities without relying on third parties (Soltani et al., 2021). In other words, the principle of SSI is that each entity owns its identity, and shares only what is necessary to authenticate itself to the system.

The SSI model has the following assumptions:

- Users must have an independent existence;
- Entities must control their own identities;
- Users must have access to their own data;

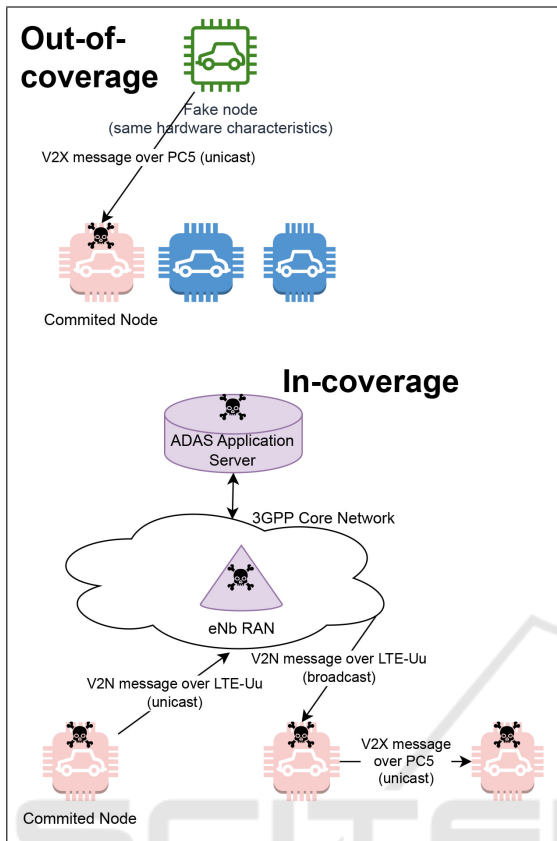


Figure 1: Diagram of the proposed threat model.

- Systems and algorithms must be transparent to the system;
- Identities must be persistent;
- Users must have a consensus on the use of their identities;
- Disclosure of claims for authentication should be minimized;
- Users' rights to privacy must be protected.

Creating an SSI identity model requires three key elements: a distributed ledger, typically a blockchain, serving as a decentralized database for recording persistent data; decentralized identifiers (DIDs), unique self-generated IDs ensuring immutability; and verifiable credentials (VCs), cryptographically secure digital versions of credentials presented to verifiers.

Within these elements, the SSI model comprises four entities: the issuer, responsible for issuing verifiable credentials; the holder, possessing a decentralized identifier and receiving credentials; the verifier, tasked with verifying credentials' validity based on evidence; and the record of verifiable data, facilitating access to the distributed ledger.

The aim is for each authentication context to have

accredited issuers authorized by the record of verifiable data. These issuers provide verifiable credentials to holders, who, during authentication, interact with verifiers. Verifiers request a proof of credential and ensure it originates from an authorized verifier, thereby verifying the user's authenticity.

The self-sovereign identity model offers secure, decentralized authentication and privacy preservation. It achieves this through two methods: selective disclosure, allowing the model to choose which credential data to reveal to verifiers while protecting unnecessary information, and Zero Knowledge Proof (ZKP), a mechanism that allows holders to prove they meet a requirement to verifiers without disclosing supporting data.

To implement the SSI model in a system, it is necessary to use an architecture. As such, Trust Over IP (ToIP) is a layered set of technical protocols and governance structures that function as a decentralized identity architecture, implementing the Self Sovereign Identity model to enable trust (Davie et al., 2019). ToIP is usually used in conjunction with SSI, as it is a faithful implementation of the model that brings the advantages of fraud mitigation, process simplification and reduced infrastructure costs.

Trust Over IP has a protocol layer stack that is followed in its architecture. It has four layers, which are divided into two categories: technology and governance.

The technology stack is divided into the following layers:

- Layer 1 - Public Utilities: This foundational layer encompasses defined utilities responsible for maintaining verifiable data records for different DID methods. These utilities store DIDs with associated public keys, utilizing diverse decentralized ledger technologies such as blockchains, distributed ledgers, decentralized file systems, or databases.
- Layer 2 - Peer-to-peer communication: Establishes wallet-to-wallet connections, which persist until one of the parties gives up. Data wallets interoperate to exchange DIDs and public keys without intermediaries.
- Layer 3 - Data Exchange Protocols: This pivotal layer in the ToIP architecture (depicted in Figure 2) focuses on issuer-verifiable credential transactions with holders. Holders get credentials verified by verifiers, leveraging issuer information accessed through the verifiable data record. To issue a verifiable credential, an issuer employs a private key for digital signing. A data wallet conducts this transaction and stores the credential

while keeping issuance private. Verification occurs using public key cryptography. Credentials are acquired by holders through issuer requests, stored in their data wallet. When a verifier seeks proof of a credential, the data wallet generates specific data proof. This proof includes the issuer's DID, enabling verifiers to verify the issuer's signature by referencing the verifiable data record and the issuer's public key. The Verifiable Data Registry (VDR) stores issuer DIDs, public keys, and cryptographic data. The VDR indexes issuer keys alongside DIDs, allowing sharing of issuer DIDs for correct public key retrieval. The VDR does not store actual credential data.

- Layer 4 - Application Ecosystem: Applications are built using DIDs and verifiable credentials to establish an ecosystem of digital trust.

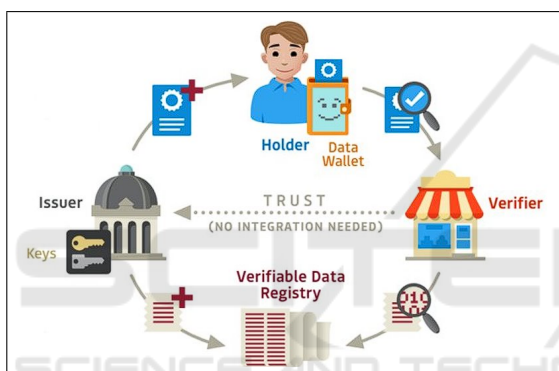


Figure 2: Entity flow in VC-based identification.

The governance stack defines the following layers:

- Layer 1 - Utility Frameworks: Governance ensures the security and integrity of verifiable data records. If a registry is operated as an authorized network, it will have a government entity responsible for its oversight.
- Layer 2 - Agent Frameworks: Government authorities set security, privacy, usability, accessibility, and data protection standards for data wallets. Agent frameworks specify trust programs, making it easier for holders to choose data wallets and agents that meet standards.
- Layer 3 - Credential Frameworks: Credentials allow holders to build trust with verifiers, as long as everyone knows the governance rules being followed. The governing authority sets policies for issuers that meet the needs, as well as rules for registering issuers and verifiers.
- Layer 4 - Ecosystem Frameworks: Governance facilitates trust between members of a digital trust

ecosystem. The governing authority is responsible for the security, privacy, and accountability of the system. Auditors can verify that members are adhering to specified frameworks.

The set of all layers seen above forms the Trust Over IP architecture, which implements the self-sovereign identity model. This framework can be used to authenticate an IoV system and to solve the proposed threat model, as shown in the next section.

## 6 SSI-BASED VEHICULAR AUTHENTICATION MODEL

As seen in the previous section, the use of a model based on Self Sovereign Identity and based on the Trust Over IP architecture can favor the decentralization of a system, as well as avoid dependence on third-party services, mainly due to the presence of the distributed ledger, based on blockchain, in the process of identifying entities.

The same concept can be applied to ADAS scenario previously discussed in threat model, with regard to the authentication of vehicles and other entities in the vehicular network. The proposed authentication scheme can be seen in Figure 3.

The ecosystem surrounding ADAS makes use of a decentralized authentication based on Self-Sovereign Identity (SSI).

A new vehicle, when in-coverage, upon registering with the ADAS application, requests a Verifiable Credential (VC) from the eNb RAN with access to the ADAS application. The eNb RAN has a DID and is coupled with a UE that acts as an issuer and verifier of credentials for the applications it has access to. The eNb RAN creates a new VC, registers the key pair with its DID in the Verifiable Data Registry (VDR), which is a distributed ledger, and returns the VC to the vehicle to be stored in its data wallet.

When this vehicle is out-of-coverage, it might receive a V2X message from a fake node with identical hardware characteristics (therefore, accepted by C-V2X architecture). The vehicle stores the message content with a "pending" flag along with the entity's VC.

Upon returning to in-coverage mode, the vehicle must update the ADAS system through V2N messages. In one of these messages, the vehicle must send the received information from the fake node, marked as pending, along with the sender's information and their VC.

The eNb RAN must access the VDR to confirm the authenticity of the message. When it decrypts the

VC with the public key, this will result in a non-existent DID. As a result, the eNb RAN rejects the message content, and it does not reach the ADAS application server, thus avoiding future decision-making errors that the server could cause.

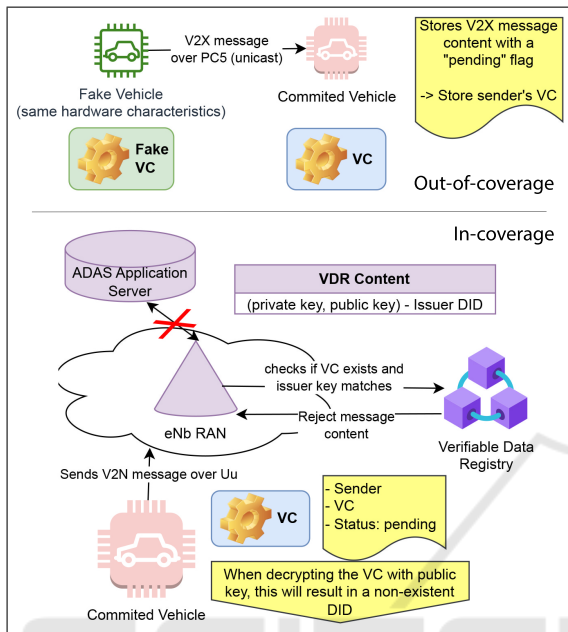


Figure 3: Authentication scheme in SSI-based IoV ecosystem for ADAS.

Although this is an open study, some research on the use of SSI in the IoV ecosystem has already been carried out, even if not in the context of authentication. (Theodouli et al., 2020) proposes an identity and trust management framework based on SSI to authenticate a software vendor API with the vehicle, aiming to improve the software update of IoT devices embedded in the vehicle. Even though it is not a study directly related to vehicular authentication in the IoV ecosystem, the research proves the possibility of using all of this framework in the context of vehicular networks.

## 7 CONCLUSION & FUTURE WORK

In brief, while the Internet of Vehicles (IoV) ecosystem is commonly regarded as secure, it contains authentication vulnerabilities that expose users to potential malicious attacks. Although researchers have developed authentication mechanisms and protocol solutions to address these concerns, none of the evaluated solutions effectively tackle the issue of maintain-

ing vehicle trust when out of network coverage, nor address the centralized nature of the default authentication mechanism. These factors introduce risks of authentication failures, as detailed in the threat model.

To confront this challenge, we proposed to apply the Self-Sovereign Identity (SSI) decentralized identity model in conjunction with the Trust Over IP architecture. This integration offers a compelling approach for implementing decentralized identification in diverse contexts. Additionally, we have discussed a proposed solution that incorporates an SSI-based authentication scheme within the IoV ecosystem, with a particular focus on ADAS applications. This solution provides a foundation for future research endeavors to explore and enhance.

## REFERENCES

- 3rd Generation Partnership Project (2017). Release 14 - 3gpp. Available in: <https://www.3gpp.org/specifications-technologies/releases/release-14>. Access in: 07/09/2023.
- Alladi, T., Chakravarty, S., Chamola, V., and Guizani, M. (2020). A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario. *IEEE Transactions on Vehicular Technology*, 69(12):14188–14197.
- Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., and Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *Ieee Access*, 8:54314–54344.
- Cui, J., Wen, J., Han, S., and Zhong, H. (2018). Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network. *IEEE Internet of Things Journal*, 5(5):3491–3498.
- Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O’Donnell, D., and Reed, D. (2019). The trust over ip stack. *IEEE Communications Standards Magazine*, 3(4):46–51.
- Gayathri, N., Thumbur, G., Reddy, P. V., and Rahman, M. Z. U. (2018). Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks. *IEEE Access*, 6:31808–31819.
- Islam, S. H., Obaidat, M. S., Vijayakumar, P., Abdulhay, E., Li, F., and Reddy, M. K. C. (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets. *Future Generation Computer Systems*, 84:216–227.
- Musleh, A. S., Yao, G., and Muyeen, S. (2019). Blockchain applications in smart grid-review and frameworks. *Ieee Access*, 7:86746–86757.
- Soltani, R., Nguyen, U. T., and An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021:1–26.
- Theodouli, A., Moschou, K., Votis, K., Tzovaras, D., Lauinger, J., and Steinhorst, S. (2020). Towards

- a blockchain-based identity and trust management framework for the iov ecosystem. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE.
- Twardokus, G. and Rahbari, H. (2022). Vehicle-to-nothing? securing c-v2x against protocol-aware dos attacks. In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*, pages 1629–1638. IEEE.
- Vasudev, H. and Das, D. (2018). A lightweight authentication protocol for v2v communication in vanets. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCOM/IOP/SCI)*, pages 1237–1242. IEEE.
- Vijayakumar, P., Azees, M., Chang, V., Deborah, J., and Balusamy, B. (2017). Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *cluster computing*, 20:2439–2450.
- Xi, N., Li, W., Jing, L., and Ma, J. (2022). Zama: A zkp-based anonymous mutual authentication scheme for the iov. *IEEE Internet of Things Journal*, 9(22):22903–22913.

