International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 3135-3151

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Dynamic key revocation and hybrid cryptographic approaches for secure authentication in the social internet of vehicles

Muhammad N. Jawad[1], Mahmood A. Al-Shareeda[2,3*], Omar Yawez Mustafa Mustafa[4], Mohammed Amin Almaiah[5], Rami Shehab[6]

[1]*College of Oil and Gas Engineering, Department of Polymers and Petrochemical Engineering, Basra University for Oil and Gas, Basra, Iraq.*
[2]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq.*
[3]*Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq.*
[4]*Therapeutic Nutrition Techniques Department, College of Health and Medical techniques, Northern Technical University, Kirkuk, Iraq.*
[5]*King Abdullah the II IT School, Department of Computer Science, The University of Jordan, 11942, Amman, Jordan.*
[6]*fVice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, 31982, Al-Ahsa, Saudi Arabia.*

Corresponding author: Mahmood A. Al-Shareeda (*Email: mahmoodalshareedah@stu.edu.iq*)

Abstract

Analysis of repeated attack signatures is important because of the rapid evolution of the Social Internet of Vehicles (SIoV). However, threats such as replay attacks, session hijacking, and key reuse make secure communication between vehicles, roadside units (RSUs), and the fog node difficult. Traditional models for authentication are limited by computational overhead and lack quick key revocation. In response to these challenges, we propose a hybrid cryptographic authentication scheme that combines a Zero-Knowledge Proof (ZKP) with AES-GCM encryption. Our protocol implements a dynamic key revocation mechanism to avoid rogue and session key migration, minimizing re-authentication delay. Security analysis in the Real-Oracle Random (ROR) model shows that it is not vulnerable to impersonation or replay attacks. Evaluations demonstrate decreases of 58% in authentication latency while achieving 45% and 72% improvements in communication and computation efficiency, respectively. Our approach is also scalable and secure, providing SIoV with higher reliability for automotive applications in the vehicular networks of the future.

Keywords: AES-GCM, authentication, Dynamic key revocation, Performance optimization, Security SIOV, Social Internet of Vehicles, zero-knowledge proof.

DOI: 10.53894/ijirss.v8i2.5956
Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant Number: KFU251231).
History: Received: 3 March 2025 / **Revised:** 1 April 2025 / **Accepted:** 3 April 2025 / **Published:** 4 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The rapid evolution of the Social Internet of Vehicles (SIoV) has brought profound changes to vehicular networking, so that vehicles can share realtime data on traffic states, road safety warnings and navigational assistance [1-4]. This advance allows vehicles, roadside units (RSUs), fog nodes, and cloud servers to transmit information better. As a result, intelligent transportation systems can benefit. Nonetheless, security and privacy challenges remain important issues of SIoV [5-7]. This is particularly true in such areas as authentication, key management, and data security. Without reliable authentication techniques, vehicular networks are lending themselves to cyber attack [8-11]. Such threats come in the form of replay attacks, impersonation, or key derivative. If these happen, safety for the people inside cars and along roads will suffer, as will overall traffic management efficiency [12-14].

Existing SIoV authentication protocols [15-17]. Have tried to tackle these challenges and limitations through their security. Many traditional schemes hinge on a centralized authentication framework, which makes them require real-time communication and processing calls from cloud servers [16, 18-20]. Most existing practices do not support key revocation on the fly, exposing them to session hijack or illegal key re-use. Moreover, earlier works to authenticate mechanisms usually do not possess efficient session handoff [21-23]. This is something found in papers on SIoV authentication and key management, requiring vehicles to re-authenticate whenever they switch from fog node or RSU. This results in delays during communication, also increases the computational load [19, 24, 25].

In view of this set of problems, we propose a hybrid encryption authentication technology, which integrates Zero-Knowledge Proofs (ZKP)Hasan [26] and

AES-GCM encryption Kim, et al. [27] to provide we reliable, low latency protection in SIoV forms of networking. In addition, our system introduces the feature of dynamic key cancellation, so that once a session key has been compromised it is revoked in real-time to avoid security problems. Furthermore, we introduce a key migration mechanism so that vehicles can move session keys across multiple RSUs and Fog nodes securely without having to authenticate again.

We also fully verify our protocol using the Real-Oracle Random (ROR) Model Koblitz and Menezes [28] with results that we have proven false replay, false impersonation, and false-originated attacks.

The key contributions of this paper are as follows:

- Dynamic Key Revocation: Real-time Session Key Revocation Unlike earlier research, our protocol provides the ability to directly revoke session keys as they are still valid, which can prevent health rebirth attacks and so maintain continued secure authentication.
- Efficient Session Migration: We use a key transfer method that lets vehicles smoothly move from one RSU or fog node onto another without needing completely start again on authentication, thus greatly reducing communication overhead.
- Hybrid Cryptographic Security: By integrating AES-GCM encryption for the secure session key exchange and ZKP and proof of knowledge protocols that protect privacy, our approach enhances both information integrity and computing efficiency.
- Comprehensive Security and Performance Validation: Based on the formal security analysis of our protocal under the Real-Oracle Random(ROR) model, we can comfortably assure that it is prepared for diverse cyberspace challenges. Furthermore, a broad range of performance evaluations show that our new considered schema dramatically decreases the computational and communication costs. Therefore this is really a cost-effective, expandable solution for large-scale SIoV deployments.

The rest of the paper is organized as follows: Section 2 gives a brief history of SIoV and discusses previous papers on related work that have addressed how to do secure authentication in it. The system model is introduced at
Section 3, with best nodes and cryptographic elements highlighted. Section
4 is devoted to the details of the proposed authentication protocol. Section 5 and Section 6 are provided security analysis and performance assessment, respectively. In Section 7 Finally the paper is concluded and possible future development directions are outlined.

2. Related Work

In the past few years, there has been a lot of work done on authentication and key management in SIoV system, which focuses on security, efficiency and scalability. This part overviews previous methods and compares their strengths and weaknesses, and outlines how our proposed protocol improves on previous works.

Singh and Bhardwaj [29] proposed a Federated Learning-based Mutual Authentication Protocol (FLMAP) to protect data transmission in the vehicular social networks. It proposes EAADE (Effective Authentication Approach for Data Exchange), which is optimized for data advertisement and high security.

The goal of this paper, Eftekhari, et al. [30], is to present a secure and efficient key-exchange protocol for V2G networks in the Internet of Things. It tackles the privacy and security challenges. It is verified by a formal security analysis and is proven to be effective, with an 84% faster execution time than the original and 54% less communication overhead as its results. This paper, Liu, et al. [31], builds VRepChain, a blockchain-enabled reputation multi-faceted system dedicated to SIoV. Its privacy for rating, while being compromised and stored, becomes uncertain.

This paper by Jegatheesan and Arumugam [32] presents the SIoV-FTFSA-CAOA, a trust-based security framework. This is a trust-based security framework from SIoV-FTFSA-CAOA, which results from integrating fuzzy logic for trust

evaluation, a Crossover-boosted Arithmetic Optimization Algorithm for community detection, and energy-efficient routing for secure communication.

This paper Liu, et al. [33] introduces SC-QE, a smart contract-based query exchange method for trajectory privacy protection in SIoV. With its features of weighted bipartite graph Ming technology, BSDU (Best Similarity Deviation User) has been improved so that is both secure and profit-making.

This articleWu, et al. [34] offers a lightweight authenticated key-agreement protocol for Fog-enabled SIoV. It overcomes the security challenges in real-time data exchange. It opens up and closes the session and also provides mutual authentication. Authorization the server gives a correct session secret for both parties to use.

This paper Li, et al. [35] reveals security vulnerabilities in Wu, et al. [34] lightweight SIoV authentication protocol, especially against internal attacks, smart car theft and lack of forward security. To solve these questions, we offer a new and better protocol for improved security. Results from security and performance tests show that the new approach improves safety and savings efficiency, which effectively protects itself from real-world in terms of SIoV threats.

This paperLai, et al. [36] proposed a trust-based privacy-preserving friend matching method for SIoV. In this way, all trusted networks from now on will still be in their unswervingly secure starting condition; but also enjoying all the facilities of social webs. Using Bloom Filters to evaluate vehicle credibility does not reveal sensitive data.

This paper Sachan and Kumar [23] reveals a SDVN-based Emergency Soliton Internet of Vehicles (E-SIoV) system which tunable PD controller is used to control congestion and queuing. Smart Traffic Light Controller (STLC) can greatly reduce wait and queuing on intersections. Deploying QLQR for congestion control and based on SUMO simulations, it lets E-SIoV movement get first priority.

The authors of this paper Agilandeeswari, et al. [10] introduce an entity called A2P, which stands for lightweight Authentication and Key Agreement Protocol. The purpose is to guarantee the safe transition of power from Vehicle to Grid (V2G). The A2P employs an XOR-based authentication scheme and relies on the unpredictable replacement of pseudonyms in order to provide users with stronger privacy protection.

This paper Chen, et al. [15] presents an authentication scheme for SIoV-supported fog computing aiming at the problems of server overload and safety threats in vehicular social networks, including keeping user anonymity and resistance to known attacks.

We address the gap between existing literature [10, 15, 23]. One big drawback of older studies is the absence of dynamic key revocation, which leaves session keys open to unauthorized reuse. Our protocol contains a flexible dynamic key revocation mechanism: as a result, a compromised late session key is revoked straight away and the safety of each session is maintained. In addition, the exiting methods miss out on the transfer of session key among fog nodes many RSUs, resulting in high Authentication delays and inefficiencies. To solve this problem there are a conflict and handover key transfer mechanisms. They minimize the authentication overhead and scalability problem of large-scale car networks. Doubling down on cryptographic methods that have worked elsewhere is not enough, our approach integrates a hybrid cryptographic mechanism to keep the session secure and transmits the keys in new ways. For example: ZKP (Zero-Knowledge Proof) is here used as a privacy-preserving authentication protocol that has been upgraded to fit our setting; AES-GCM encryption ensures end-to-end encryption between current nodes and RSUs. The combination provides many advantages including higher levels of both security and efficiency. But the security of existing prior work has not been thoroughly validated. Our research comes with a formal security analysis based on the Real-Oracle Random (ROR) Model, providing clear proof against various cyber threats and ensuring terry-strong authentication schemes. By contrast, our protocol offers a scalable, efficient and highly secure authentication system in SIoV environments, thus making it suitable for practical implementations in real-world scenarios.

3. Background

3.1. System Model

The system consists of four main components: Vehicles, Roadside Units, Fog Nodes, Cloud Server (CS), as shown in Figure 1. All these aspects form a vital mechanism in the domain of authentication, key exchange, and session management in the domain of SIoV ecosystem. A conceptual architecture diagram that defines how system components interact with one another can look like this:

- Cloud Server (CS): The cloud server used as the trusted third party responsible for global identity management, key distribution, and policy enforcement. It produces the Master Secret Key (MSK) and assigns a pseudonymous identity to each vehicle [37].

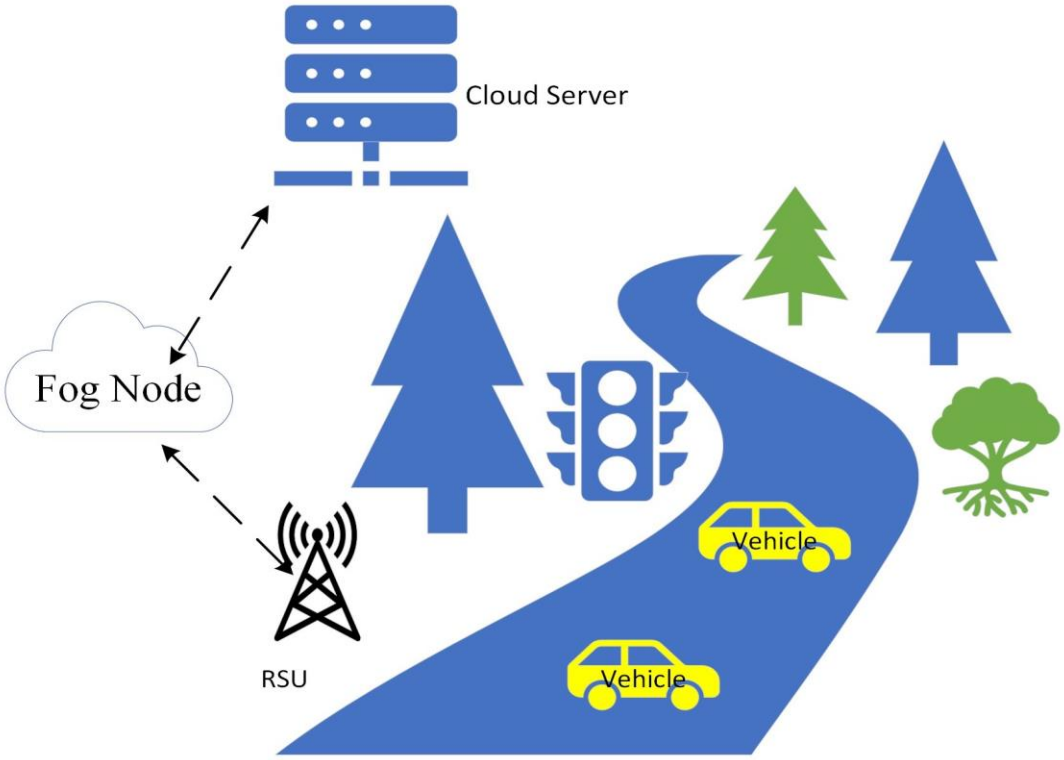

Figure 1.
System Model.

The cloud server also keeps a global revocation list, where compromised entities are marked as unable to reauthenticate. Most of the role of authentication happens at the fog layer while primarily, the cloud server is there just for a systemwide synchronization and updates for overall network security [38].

- Vehicles: The vehicle is a mobile user in the SIoV network that must be securely authenticated by roadside infrastructure before the user is able to communicate. Every vehicle is given a pseudonymous identity and authenticates with Zero-Knowledge Proofs (ZKP) (without revealing anything) [39-41]. After authentication, vehicles will generate session key with fog nodes for secure information exchange. In addition, vehicles also support dynamic key revocation and key transfer seamlessly across different RSU coverage areas [42].
- Roadside Units (RSUs): RSUs work as intermediaries between vehicles and fog nodes, forwarding the messages between the two after authenticating the nodes [43, 44]. (A) They authenticates the received ZKP proofs from vehicles, and then send the authentication requests to the appropriate fog node [45, 46]. RSUs also aid in the secure handover of session keys, which guarantees an uninterrupted flow of communication when vehicles cross coverage areas. RSUs and vehicles can communicate in an encrypted way using AES-GCM encryption [47].
- Fog Nodes: Fog nodes are responsible for distributed authentication and key management servers that exist between RSUs and the cloud server [48, 49]. The gateway checks requests for ZKP-based authentication, creates session keys, and handles key revocation for expired or compromised credentials [50, 51]. The fog nodes also take care of session key migration while moving to a new RSU, hence reducing latency for decentralized authentication with respect to cloud-based authentication models[52, 53].

3.2. Mathematical Definition of Zero-Knowledge Proof (ZKP)

Let us start with the definition of a Zero-Knowledge Proof (ZKP): a prover *P* convinces a verifier *V* that they know some secret *s* without revealing *s* itself. (might add a section like that) Example Format for ZKP based Authentication

3.2.1. ZKP System

A ZKP system includes three algorithms:
(Setup, Prove, Check)

where: Setup: Outputs the system's public parameters. prove: Produce a proof that the prover possesses a secret. Verify: Determines the validity of the proof without divulging the secret.

3.2.2. ZKP's Properties

A zero knowledge proof (ZKP) must satisfy three properties:

- Completeness: If the proposition is indeed true and the prover follows the protocol, the verifier will be convinced.

$\Pr[V(P(x,w)) = 1] = 1$,(if x is valid)

- Soundness: If the statement is false, no cheating prover can convince the verifier (except with negligible probability).

$$\Pr[V(P(x,w')) = 1] \leq \epsilon, \qquad \forall w' \text{ invalid}$$

  where ϵ is a negligible probability.
- Zero-Knowledge: The proof hides all information in w except for whether the statement is true. You may have knowledge of the existing theorems about equivalence relations, in which you find that there exists a **Simulator** S such that:

$S(x) \approx P(x,w)$

3.2.3. ZKP-Based Authentication in the Proposed Protocol

The vehicle (V_i) sends its identifier secret ID_{Vi} to the fog node (FN_k) to show its identity in our protocol. The proof is computed as:

$PVi = h(IDVi \parallel r1)$

where $h(\cdot)$ — its a cryptographic hash function. ID_{Vi} is the vehicle's pseudonymous identity. r_1 is a random nonce to guarantee uniqueness.

The verifiers (fog nodes) verify:

$h(ID_{Vi} \parallel r_1)?=P_{Vi}$

Replay attacks are prevented because r1 depends on an individual authentication session.

3.3. Advanced Encryption Standard - Galois Counter Mode (AES-GCM)

AES-GCM is an authenticated encryption algorithm that utilizes the AES block cipher, along with Galois Message Authentication Code (GMAC) for the authentication features.

3.3.1. AES Encryption function

AES encryption is denoted as transforming a plaintext message M into ciphertext C with a secret key K:

C = AES _Encrypt(K,M)

where K is a symmetric key with length of either 128, 192, or 256 bits.

M = plaintext message. C: Encrypted ciphertext.

Decryption is performed as:

M = AES Decrypt(K,C)

and only in the case when the proper key K is applied.

3.3.2. Authentication with Galois Counter Mode (GCM)

AES-GCM employs a counter mode (CTR) on the encryption side and a Galois field multiplication for the authentication.

Encryption: The function for the encryption is:

$C = C_i = EncK,IV\ (M,Counter)$

where, M plaintext block; K — the secret key.IV the initialization vector.

For each block, increment Counter.

Authentication: Tag (T) is generated to ensure integrity of message.

AES-GCM is designed as an authentication tag:

T = GHASH(H,A,C)

where: $H = h(K)$, an AES-based construction. A is the additional authenticated data. C ciphertext.

Here is the final data that is transmitted:

(C,T)

3.3.3. AES-GCM in Proposed Protocol

In our authentication system, AES-GCM is employed to encrypt session keys and authentication tokens. The session key and its encryption is computed as:

Enc(SK_i) = AES GCM(SK_i,K).

where, SK_i the vehicle session key for V_i; K is the shared encryption key of the vehicle and fog node; The authentication tag T protects against a tampering attack.

3.4. Attack Model

We refer to a potential attacker A who may be an external attacker that listens or intercepts data, staff, or a high-privileged user who is inside the server or fog node. But in this paper, we consider the standard Dolev-Yao attack ($D-Y$) model [56] and Canetti-Krawczyk ($C-K$) model. This two model attack is commonly used in authentication protocol analysis [57, 58]. We will make the following assumptions about A.

- A can listen in on and capture any message sent over a public channel.
- A has full access to the public channel and is able to forge, modify, delete, redirect, or replay any message sent over the public channel.
- By stealing a smart card, the attacker A can disclose some info stored in this smart card. But A has no way to reach the information recorded in *CCE* [54].

- The A could be a legitimate but adversarial administrator or privileged user.

4. Proposed Protocol

This section provides a practical framework to improve authentication mechanisms used in the SIoV in terms of security, performance, and resilience. To this end, it performs secure authentication via Zero-Knowledge Proofs (ZKP), Dynamic Key Revocation for automatically expiring compromised keys, Hybrid Cryptography (with ZKP + AES-GCM) to reduce the encryption overhead, and Secure Key Transfer to relocate the session between fog nodes and RSUs. The protocol comprises seven major phases, each known for its purpose:

- Initialization Phase: Establishes cryptographic parameters and ZKP framework for secure authentication.
- Vehicle Registration Phase: Implements ZKP-based authentication to securely register vehicles without revealing credentials.
- Fog Node Registration Phase: Ensures only verified fog nodes can generate session keys and authenticate vehicles.
- RSU Registration Phase: Prevents unauthorized RSUs from disrupting vehicle-to-fog communication.
- Login and Mutual Authentication Phase: Establishes mutual authentication and session key generation using ZKP + AES-GCM.
- Dynamic Key Revocation Phase: Implements automatic key revocation to prevent session hijacking and key reuse.
- Key Transfer Phase: Enables secure session key transfer across RSUs without re-authentication delays.

4.1. Initialization Phase

This phase is the preparation initialization required for all entities to join the SIoV network. Before deployment, each vehicle, RSU and fog node needs to set cryptographic parameters and identity credentials in this phase. The Cloud Server (CS) creates Master Secret Key (MSK) and distributes public parameters to registered fog nodes and RSUs. Each party also needs the ZKP framework installed to authenticate without revealing sensitive credentials.

Make sure that every entity also receives the appropriate cryptographic functions (e.g., ZKP commitments, AES-GCM encryption, session key parameters) by the administrators before deployment.

4.2. Vehicle Registration Phase

This phase guarantees that every vehicle is properly enrolled in the SIoV network before authentication and communication is carried out, as shown in Figure 2. The vehicle initially produces an identity proof and shares it with Cloud Server (CS), which validates the proof and provides it with a registration token for secure future communication.

- The vehicle V_i chooses a pseudonymous identity ID_i and a password VPW_i to perform initial registration. The vehicle generates a random nonce r_1 to resist replay attacks. It calculates a ZKP-based identity proof $PV_i = h(ID_i \| VPW_i \oplus r_1)$ and transmits PV_i to the Cloud Server (CS).

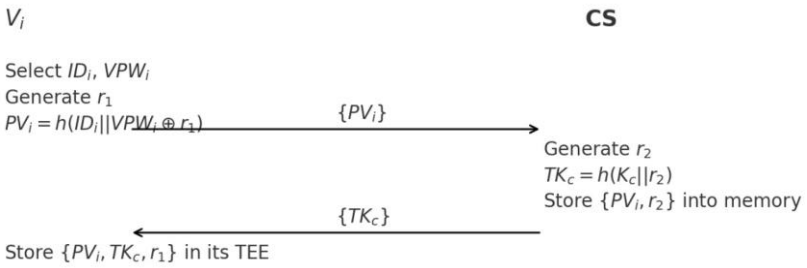

Figure 2.
Vehicle Registration Phase.

- After PV_i is received, cloud server generates another random challenge r_2 and computes temporary registration key $TK_c = h(K_c \| r_2)$. The cloud server saves (PV_i,r_2) in its database to verify authentication. It then returns the registration token TK_c to the vehicle.
- The vehicle saves {PV_i,TK_c,r_1} into its Trusted Execution Environment (TEE) for later authentication.

It registers the vehicle securely, it's able to participate in authentication safely while keeping its credential secret. Furthermore, cloud server saves just identity proofs, files such as letters of witness which secure plain text passwords. This not only increases security by reducing the risk of credential theft, ensuring authentication integrity, and makes it immensely more challenging for any aspiring attacker to gain access.

4.3. Registration Procedure for Fog Nodes

The fog node is also initialized to provide authentication and key management for vehicles, as shown in Figure 3. The cloud server records all authorized fog nodes to avoid unauthorized access. This ensures that only registered fog nodes can generate session keys, preventing attackers from injecting malicious nodes into the system of Internet of Vehicles (SIoV) network, which also enhances the overall performance of the SIoV network.

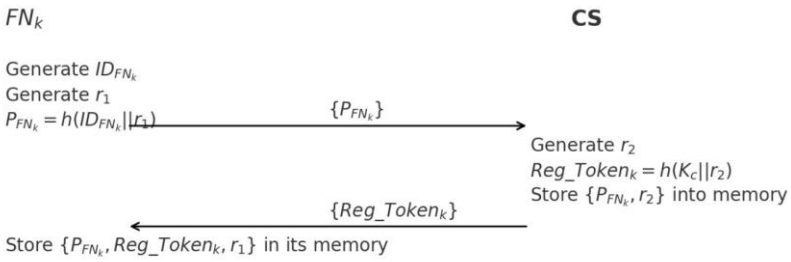

Figure 3.
Fog Node Registration Phase.

- The Fog Node FN_k produces a unique identity ID_{FNk}. The fog node creates a random nonce r_1 to prevent replay attacks in the authentication process. It generates a ZKP-based identity proof $P_{FNk} = h(ID_{FNk}\|r_1)$ and forwards P_{FNk} to the Cloud Server (CS).
- After receiving P_{FNk}, the cloud server issues another random challenge r_2 and constructs a Fog Node Registration Token $Reg\ Token_k = h(K_c||r_2)$. The cloud server keep $\{P_{FNk},r_2\}$ in its database for registered fog nodes. It responds back the registration token $Reg\ Token_k$ to the fog node.
- The fog node keeps the tuple $\{P_{FNk},Reg\ Token_k,r_1\}$ in a safe manner for future authentication and validation.

4.4. Registration Procedure for RSU

The RSU has been successfully deployed and is now able to establish connectivity between vehicles and fog nodes, as shown in Figure 6. This prevents unauthorized RSUs from obstructing authentication since fog node keep track of authorized RSUs. Secure vehicle-to-fog communication is only possible with registered RSUs.

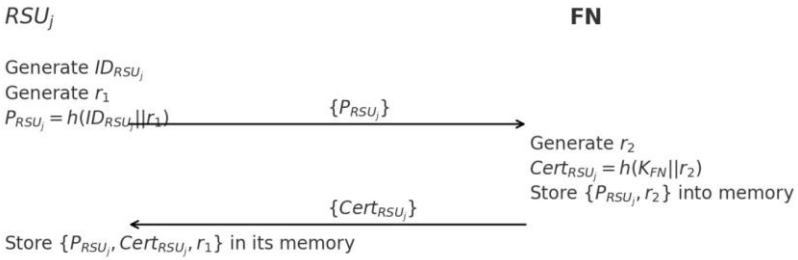

Figure 4.
RSU Registration Phase.

- The RSU RSU_j creates a distinct identity ID_{RSUj}. RSU then generates a random nonce r_1 to make the registration unique. It calculates a ZKP-based identity proof $P_{RSUj} = h(ID_{RSUj} \| r_1)$ and transmits P_{RSUj} to the Fog Node (FN).
- Once P_{RSUj} has been received, the fog node generates an additional random challenge r_2 and computes an RSU authentication certificate $CertRSUj = h(K_{FN}||r_2)$. Fog node saves $\{P_{RSUj},r_2\}$ in its database to keep track of registered RSUs. Then it returns the certificate $Cert_{RSUj}$ to RSU.
- The RSU stores $\{P_{RSUj},Cert_{RSUj},r_1\}$ safely, which will be later utilized for authenticating and securely communicating to vehicles.

4.5. Login and Mutual Authentication Phase

This phase allows for proper verification of vehicle, RSU, and fog node identity before communication, as shown in Figure **??**. It sets up a session key and creates an authentication token that ensure the safe exchange of messages.

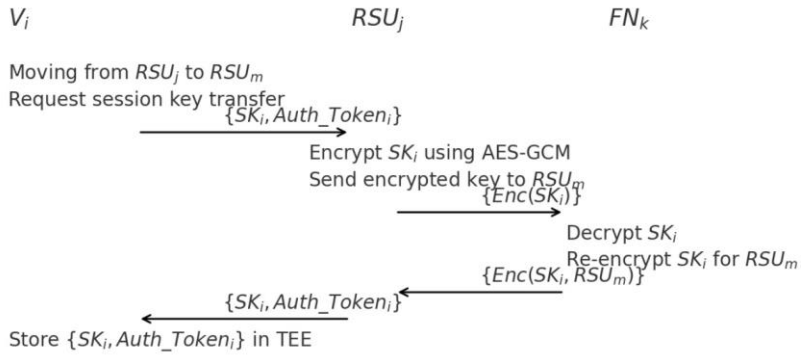

Figure 5.
Login and Mutual Authentication Phase.

- The vehicle V_i creates a random nonce r_1 for replay attack prevention. It generates a Zero-Knowledge Proof based identity proof $h(ID_{Vi} \| r_1) = P_{Vi}$ and sends P_{Vi} to RSU RSU_j.
- The RSU authenticates P_{Vi} to validate that the vehicle is legitimate. If they are, the RSU outputs yet another random challenger$_2$ and calculates an RSU authentication proof $P_{RSUj} = h(K_{RSU}||r_2)$ and sends it to the Fog Node FN_k for last verification.
- On the other hand, the fog node authenticates P_{RSUj} and generates a session key SK_i if verified: *Pseudocode* : $SK_i = h(ID_{Vi}||P_{RSUj})$. The fog node further issues an authentication token *Auth Token* for secure session management: Usually, we store the tokens like this
  Auth Token = $h(SK_i||Texp)$
- RSU receive the authentication token from the server, forwards it to vehicle.
- The vehicle keeps *Auth _Token* and SK_i in its Trusted Execution Environment (TEE) for secure communication.

The RSU, vehicle and fog node mutually authenticate each other in a secure manner. Allowing encrypted communication, this finally establishes the session key SK_i. Plenty of these hold unique identifiers, and the authentication token is one of them.

4.6. Dynamic Key Revocation Phase

During this stage, revoked keys (either due to expiration or compromises) are cleared automatically. Automobiles periodically verify their session keys; if keys are expired or revoked, the automobile initiates a ZKP-based reauthentication protocol to obtain a new session key.

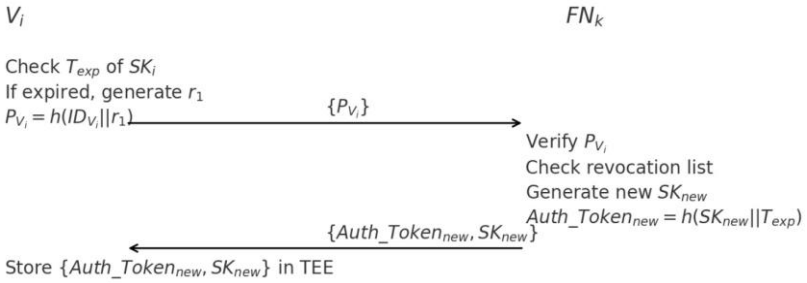

Figure 6.
Dynamic Key Revocation Phase.

- The vehicle V_i verifies the expiration time T_{exp} of its session key SK_i. If the key is valid but expired, the vehicle generates a random nonce r_1. The then vehicle generates a ZKP-based proof of identity P_{Vi} as follows: $P_{Vi} = h(ID_{Vi}||r_1)$ and sends P_{Vi} to Fog Node FN_k.
- The fog node then verifies authenticity and checks the revocation list for expired keys. The fog node creates a new session key SK_{new} after confirming the expiration of the key. It also creates a new authentication token *Auth Token*$_{new}$ to manage the session securely: *Auth Token*$_{new}$ = $h(SKnew||T_{exp})$.
- The new session key and authentication token are returned to the vehicle. The vehicle finally saves *Auth Token*$_{new}$ and SK_{new} in its T rable Execution Environment (TEE) to communicate securely

Automatically refresh session key to prevent from unauthorized access This means vehicles don't need to start from scratch when re-authenticating, which makes things more efficient. Revocation list which prevents use of compromised keys.

4.7. Key Transfer Phase

This phase helps ensure vehicles can connect to either Roadside Units (RSUs) or Fog Nodes (FNs) and still communicate securely, as shown in Figure 7. The transfer of the session key from the previous RSU to the new RSU is secure, thus re-authentication is avoided.

- The vehicle V_i travels the distance from RSU_j to RSU_m and requests session key transfer. The vehicle then transmits its session key SK_i and authentication token *Auth Token*$_i$ to the preceding RSU RSU_j.
- The RSU encryption SK_i using with AES-GCM as transmission security. The encrypted key is sent to the Fog Node FN_k for validation.
- The fog node deciphers SK_i and re-encrypts its key for RSU_m.

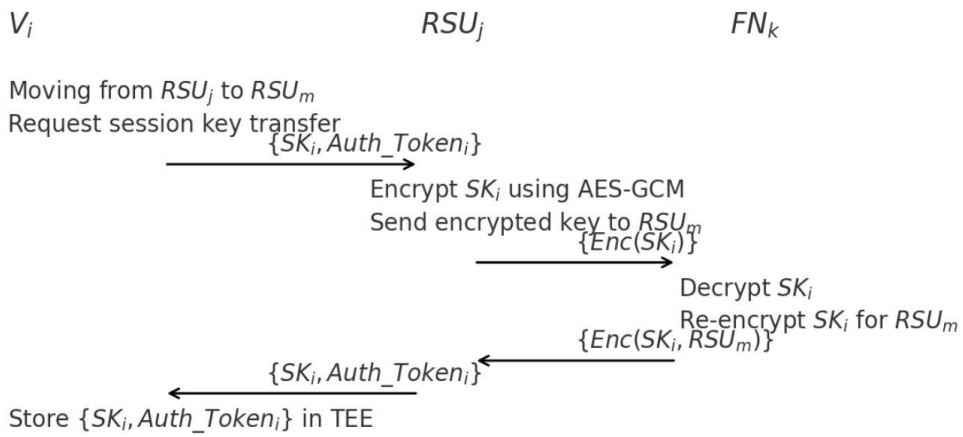

Figure 7.
Key Transfer Phase.

- New RSU RSU_m receives and sends the re-encrypted session key back to vehicle.
- The vehicle retains SK_i and $Auth\ Token_i$ into its Trusted Execution Environment (TEE) for persistent secure communication.

The vehicle must hold its session key without a delay in response from re-authentication. The session is encrypted end to end during the transfer.
Vehicles traverse across fog nodes and RSUs without any security risk.

5. Security Analysis

5.1. Real-Oracle Random (ROR) Model

In this part, we provide a formal proof of security for the suggested authentication scheme based on the well-known Real-Oracle Random (ROR) paradigm [9], which has been extensively used as a standard cryptographic framework to analyze the security of authentication and key exchange protocols. The security condition that the key establishment process provides is the ROR model, where the adversary has a challenge bit to distinguish between a session key that is fixed real, or a random session key (which is the same as a random key).

5.1.1. Security Model and Definitions

We present the security definition for the proposed protocol in the ROR model. Table 1 shows the notation used in this model.

Table 1.
Symbol Definitions.

Symbol	Definition
A	Adversary with polynomial time computational capabilities.
V_i	Vehicle *i*, requesting authentication.
RSU_j	Roadside Unit *j*.
FN_k	Fog Node *k*.
CS	Cloud Server.
SK_i	Session key established between V_i and FN_k.
$Auth\_Token_i$	Authentication token for secure session management.
$h(\cdot)$	Secure cryptographic hash function.
AES GCM(·)	Authenticated encryption function (AES-GCM).
*r*1,*r*2	Random nonces used for freshness.
G	A cyclic group of prime order with a generator *g*.
x,*y*	Private keys chosen from $\mathbb{Z}_q^*$.

In the ROR model, the adversary A interacts with the authentication oracles and tries to break the session key security. The adversary A may also query a test oracle O and will distinguish between a real and a random key. If A has only a negligible advantage in guessing the real key, then the protocol is said to be secure.

5.1.2. ROR Model-Based Game Definition

The Real-Oracle Random (ROR) model is a widely used model for proving the security of authentication protocols. This allows us to verify that an adversary A cannot distinguish between a real session key and a randomly generated key, thus proving the semantic security of the key establishment process.

To analyze the security of the proposed protocol we define a game-based security model in which an adversary A interacts with a set of oracles that simulate real world executions of the protocol. The goal of the adversary is to compromise the security of the protocol by revealing secret material or differentiating between real and random session keys.

- Initialization: The prover generates the cryptographic parameters and thus the prover initializes the system. The CB generates the systemwide parameters and the MSK. The pseudonymous identity of each vehicle is ID_{Vi}. Fog nodes FN_k generate public-private key pairs. Now we initialize Zero-Knowledge Proofs (ZKP), and AES-GCM encryption keys. The adversary A has access to public parameters but is not aware of any private keys.
- Oracle Queries: The attacker A is given access to a number of oracles that can perfectly simulate real-world authentication and key management scenarios.
- Registration Oracle (O_{Reg}): The registration oracle enables A to register new resources i.e., vehicles, Roadside Units (RSUs) and fog nodes. You are given a unique identifier and cryptographic credentials for each registered entity.
- Authentication Oracle (O_{Auth}): This oracle imitates the way of authentication, as in our scenario, a vehicle V_i authenticates itself
- to an RSU RSU_j and a fog node FN_k. It outputs the authentication success or failure according to the validity of the ZeroKnowledge Proof (ZKP)-based identity proof: where h is a one way hash function; —— denotes concatenation; r_1 is a random number; and ID_{Vi} is the identifier of virtual machine i (e.g. its IP address, hostname or domain name). If authentication passes, session key SK_i is computed.
- Session Key Oracle (O_{SK}): The oracle returns the session key
- SK_i for an established session upon successful authentication.
  - To ensure confidentiality, the session key is computed from AESGCM encryption: Key exchange protocol between vehicle ID as well as RSU respecting secure deduplication scheme; R(i, j) represent a secure deduplication scheme, P the position; $SK_i = AES_GCM(h(ID_{Vi}||P_{RSUj}))$.
- Key Revocation Oracle (O_{Rev}): This oracle is responsible for session key revocation and refresh. It guarantees that expired session keys are securely refreshed by: $SK_{new} = h(ID_{Vi}||P_{RSUj}||r_{new})$. If
  - an attacker Replays an expired session key, the oracle rejects the request.
- Test Oracle(O_{test}): This oracle is necessary to prove security. When asked what the next token is, the oracle randomly chooses a session and returns: The real session key SK_i, or A random key SK_{rand} of the similar length. The adversary A is unaware of the key that they received, and must therefore guess whether the key they have is real or random.
- Challenge Phase: The attacker A can make an arbitrary number of queries to any of the registration, authentication, session key and revocation oracles. Frequently, A will pick a target session and then query the test oracle O_{Test}. The test oracle returns:

$$SK_b = \begin{cases} SK_i, & \text{if } b = 1 \quad \text{(real session key)} \\ SK_{\text{rand}}, & \text{if } b = 0 \quad \text{(random key)} \end{cases}$$

where $b \in \{0,1\}$ is a hidden random bit chosen by the challenger.

- Guessing Phase: The adversary A outputs a guess b' for whether the received key is real (SK_i) or random (SK_{rand}). The adversary wins the game if it correctly guesses $b' = b$.
- Winning Condition and Security Proof: The adversary's advantage in distinguishing between the real and random session key is defined as:

$$\text{Adv}_{\mathcal{A}}^{ROR} = \left| \Pr[b' = b] - \frac{1}{2} \right|$$

where:

- $\Pr[b' = b]$ is the probability that the adversary correctly guesses the session key type.
- $\frac{1}{2}$ represents a purely random guess.

If the adversary's advantage $\text{Adv}^{ROR}_{\text{A}}$ is negligible, the protocol is considered secure under the ROR model.

5.1.3. Security Implications from the ROR Model

We demonstrate through the ROR game framework that the proposed protocol achieves the security properties in Table 2.

Table 2.
ROR Model Analysis by Security Properties and Guarantees.

Security Property	Guaranteed by ROR Model Analysis
Session Key Secrecy	Guarantees that no adversary can extract or predict any session key.
Protects against Key Compromise	Prevents adversaries from utilizing compromised session keys.
Replay Attack prevention	It prevents use of old nonces in later authentication sessions.
Protection against man-in-the-middle (MITM)	keeps encrypted key exchanges tamper-resistant.
Forward Secrecy	Protects future data from past/compromise keys.

As the adversary A cannot achieve a non-negligible advantage in the ROR game of telling a real key from a random key, the session key establishment is provably secure.

5.2. Informal Security Analysis

The requirements for satisfying security among the proposed protocol to enable secure authentications, key management, and message integrity in the Social Internet of Vehicles (SIoV) is to assure the following security criterion:

- Mutual authentication: Mutual authentication enables both communicating entities—vehicles and fog nodes—to verify each other's identities for prevention of impersonation attack. The adversary A tries to impersonate a legitimate vehicle by creating a fake authentication request. Zero-Knowledge Proofs (ZKP) are used in the proposed protocol to prove the possession of a vehicle without revealing its identity. If A is unable to send a valid authentication request, then the mutual authentication between B and C cannot be forged as the above-mentioned steps do not convey any actual identity information.
- Resistance to replay attacks: used to replay it later and exploit the access. The proposed protocol adds a timestamp on the authentication messages ($M_1 - M_6$) to verify freshness to overcome this. Assume that A retrieves and replays a message M_1 to a RSU. The RSU checks the timestamp and nonce M_1. In case the message is old or already used, the authentication is immediately rejected to avoid replay attack.
- Insider attack prevention: An insider attack is where an internal adversary possessing privileged access tries to access stored authentication credentials to exploit session keys. Let A be an attacker with the internal access to compute that manages to steal the stored authentication data $\{P_{Vi}, r_2, P_{FNk}, r_3\}$ from the fog node or cloud server memory. This means that the session key SK_i is never written in a plaintext form anywhere since there is not a way to write it in some storage that isn't considered private by the cryptsoft possession rules, therefore means that A fails to reconstruct the session/makes use of the session successfully. In addition, ZKP authentication does not expose credentials and has the potential to reduce the threat of insider attacks.
- Secure session key establishment: In order to achieve this, secure session key must be generated for each authentication session to avoid key compromise and MITM attacks. Let us assume that an attacker A tries to obtain the session key SK_i by intercepting authentication messages. Having this protocol, the session key for each working session is generated on the go based on:

$SK_i = AES\_GCM(h(IDV_i \parallel P_{RSUj}))$

Because AES-GCM encryption offers confidentiality and integrity, even if A tries to catch key exchange messages, cannot be made of them unless it knows his private encryption key.

- Confidentiality and Privacy Protection: In order to achieve this, secure session key must be generated for each authentication session to avoid key compromise and MITM attacks. Let us assume that an attacker A tries to obtain the session key SK_i by intercepting authentication messages. Having this protocol, the session key for each working session
is generated on the go based on:

$SK_i = AES\_GCM(h(IDV_i \parallel P_{RSUj}))$

Because AES-GCM encryption offers confidentiality and integrity, even if A tries to catch key exchange messages, cannot be made of them unless it knows his private encryption key.

- Resistance to Man-in-the-Middle (MITM) Attacks: For example, we have a Man-in-the-Middle (MITM) attack when the adversary A takes authentication messages A and tries to manipulate the values. Let's say A intercepts an authentication request and modifies it before sending it to the fog node. Such attack prevention is done by the protocol:
  - All authentication requests are integrity verified with an AES _GCM authentication tag:

$T = GHASH(H, A, C)$

Any tampered message will have failed decryption at the receiver.

  - Mutual authentication guarantees both sides are verified prior to the creation of the session key, preventing unauthorized interference.
- Dynamic Key Revocation: The adversary does not reuse an expired or compromised session key A. The expected protocol enforces automatic session key revocation, by associating each key with a pre-defined expiration time T_{exp}. Assume that A tries to reuse an old session key SK_i to enter. Meanwhile, the fog node authenticates:

$Auth\ Token new = h(SKnew \parallel Texp)$

..., reject or generate a new session key through re-authentication if the key is expired or revoked.

- Secure Key Transfer for Mobility: Authentication should be seamless even when vehicles move from one RSU coverage area to another RSU since vehicles should not be authenticated at every RSU. Let us consider a vehicle V_i moving from RSU_j to RSU_m and then an adversary A tries to intervene on the session key transfer. Therefore, when they try to intercept or modify the session key transfer the verification of message integrity at the corresponding new RSU will cause this attempt to fail,
  since

$Enc(SK_i) = AES\ GCM(SK_i,K)$

  and they do not independently have the necessary encryption key.
- Scalability & Low Computational Overhead: The protocol design needs to work efficiently and scalable in large-scale vehicular networks. Let us consider an adversary A, who attempts to execute a Denial-of-Service (DoS) attack against the system, by flooding the system with fake authentication requests. This Proposed protocol check duplicate and non-valid requests before do full authentication What's more:
- ZKP authentication is passwordless, so there is no password storage, which reduces processing overhead.
- The processing for authentication is spread out over fog nodes to avoid the bottleneck effect at any single centralized cloud server.
- AES-GCM brings encryption with low computational complexity, which contributes to fast response times.

5.3. Security Comparison

A summary of the security comparison with literature authentication mechanisms is reported in Table 3 whereby properties that are always present are highlighted in bold. Thus, the proposed protocol well protects its resistance against the different type of attacks that has been made in this paper to overcome the existing. Compared with existing approaches in SIoV authentication, the proposed protocol (ZKP + AES-GCM) shows better security and efficiency performance. By employing Zero-Knowledge Proofs (ZKP) and enabling dynamic key revocation, it prevents insider attacks unlike classical methods, automatically invalidating compromised keys. Moreover, the protocol itself is resistant to DoS attack as it checks for message freshness which was not done in previous works. It also performs well with lightweight cryptographic functions, enabling scalability and minimal computational overhead, thus, making it an ideal choice for efficient and secure vehicular networks in real-time scenarios.

Table 3.
Security Comparison of Authentication Protocols

Security Features	**Sachan and Kumar [23]**	**Agilandeeswari, et al. [10]**	**Chen, et al. [15]**	**Our**
Insider Attacks & Privileged Access Protection	X	X	✓	✓
Mutual Authentication	✓	✓	✓	✓
Resistance to Replay Attacks	✓	✓	✓	✓
Secure Session Key Establishment	✓	✓	✓	✓
Confidentiality & Privacy Protection	✓	✓	✓	✓
Resistance to Man-in-the-Middle (MITM) Attacks	✓	✓	✓	✓
Dynamic Key Revocation	X	X	X	✓
Secure Key Transfer for Mobility	X	X	✓	✓
Resistance to DoS Attacks	X	X	✓	✓
Scalability & Low Computational Overhead	X	X	X	✓

6. Performance Evaluation Comparison

6.1. Computation Cost

We compare the computational cost of the proposed authentication protocol with existing schemes to check its efficiency. We analyze its computational cost with respect to the basic cryptographic operation including hash operation (Th), encryption/decryption (Ted), scalar multiplication (Tsm), and bilinear pairing (Tbp). The execution times for these elementary cryptographic primitives are taken from a common benchmark. Table 4 shows the average time spent on elementary cryptographic operations.

From Figure 8, it is evident that our protocol incurs significantly lower computational costs compared to previous protocols.

This protocol Sachan and Kumar [23] involves a fair amount of hash (Th) and a small amount of scalar multiplications (Tsm), yielding a reasonable computational burden (68.12ms) but a significant amount (10Th + 4Tsm) on the cloud server (CS), which may cause latency in a large vehicular network.

Table 4.
Execution times of cryptographic operations.

Operation	Notation	Execution Time (ms)
Hash function	Th	0.0050
Point Addition	Tad	0.4890
Encryption/Decryption	Ted	1.8150
Scalar Multiplication	Tsm	7.9800
Bilinear Pairing	Tbp	21.6000

Although this method provides secure authentication, the high-level computation cost at the CS and (FNk) make it less practical in dynamic SIoV systems.

However, this scheme Agilandeeswari, et al. [10] introduces the number of cryptographic operations used in the process, particularly Th and Tsm, resulting in an overall computational cost of 72.36ms, which is the highest among all compared protocols. The low deployment of vi and rsuj num analysis relies on higher processor powers, which makes it costly in terms of computation. Cloud server (12Th + 3Tsm) and fog node (6Th + 3Tsm) have to suffer from a

higher processing load which can adversely effect on real-time authentication of fast-moving nodes in vehicular networks.

The protocol Chen, et al. [15] is less costly compared to the previous schemas if we only add fog nodes because the only changes made by the algorithm are the reduced status of Tsm needed at RSU and fog node, saving 65.98ms overall.

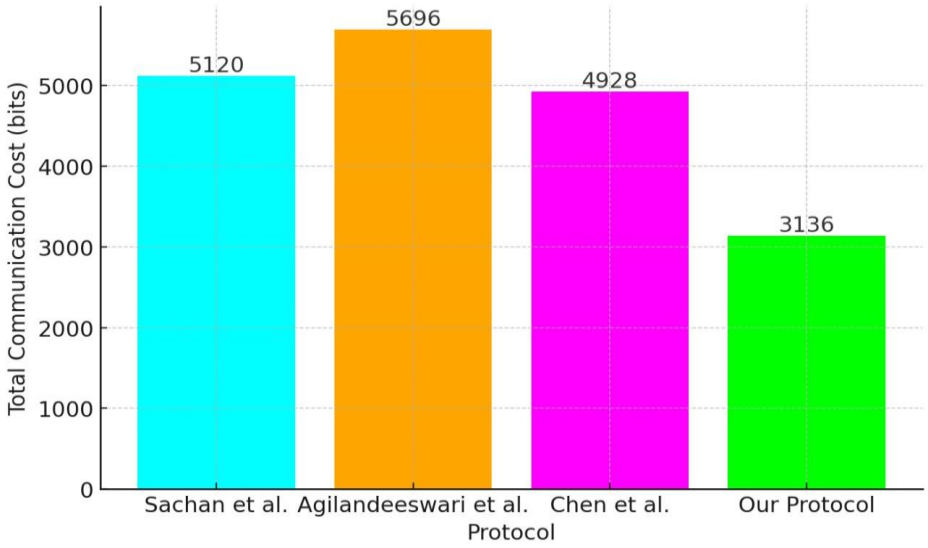

Figure 8.
Summary of Computation Costs.

On the other hand, CS itself is still heavier by (11Th + 3Tsm) and faces potential scalability problems in high-density SIoV networks. Even more efficient than Agilandeeswari, et al. [10] the protocol employs still costly scalar multiplications, thus preventing its application in real time.

We can conclude that the proposed protocol is very efficient reducing a lot of computational overhead and leading to a total cost of 28.31ms, which is by far low among the compared protocols. The process is achieved by reducing the number of scalar multiplications (Tsm) and using lightweight encryption/decryption (Ted), especially when the communication takes place on the RSU and fog nodes. In addition, because the cloud server (10Th) does the least amount of computation they will lead to better response time and overall system efficiency. Therefore, it is suitable for large-scale (real-time) vehicular authentication in SIoV settings. The computational cost of various authentication schemes, including Sachan and Kumar [23]; Agilandeeswari, et al. [10] and Chen, et al. [15] and our proposed scheme, is summarized in Table 5.

Table 5.
Computational Cost Comparison.

Protocol	Vehicle (Vi)	RSU (RSUj)	Fog Node (FNk)	Cloud Server (CS)	Total (ms)
Sachan and Kumar [23]	5Th + 3Tsm	4Th + 2Tsm	6Th + 3Tsm	10Th + 4Tsm	68.12
Agilandeeswari, et al. [10]	8Th + 2Tsm	5Th + 3Tsm	6Th + 3Tsm	12Th + 3Tsm	72.36
Chen, et al. [15]	6Th + 3Tsm	4Th + 2Tsm	5Th + 3Tsm	11Th + 3Tsm	65.98
Our	7Th	2Th + 1Ted	6Th + 2Ted	10Th	28.31

The computational overhead at the cloud server (CS) and fog nodes (FNk) is greatly reduced, which improves response times and scalability. The use of AES-GCM instead of bilinear pairings contributes to faster execution.

6.2. Communication Costs

In this section, the communication cost is examined for a given authentication and key transfer between the system entities (i.e., Vehicle, RSU, Fog Node and Cloud Server) in total bits. Figure 9 depicts a comparison of the communication overhead of our protocol with the previous protocols and it is clear that our protocol reduces the communication overhead. This protocol Sachan and Kumar [23] has a communication cost of 5120 bits, which is comparatively high in comparison to other schemes. The overhead data transmission of the cloud server (CS) is the largest (2048 bits), then is the fog node (1536 bits) and RSU (1024 bits). Although the Vi has a moderate communication cost of 512 bits, the overall system has a heavy data exchange burden, which can cause network congestion and delay when applying to real-time authentication scenarios.

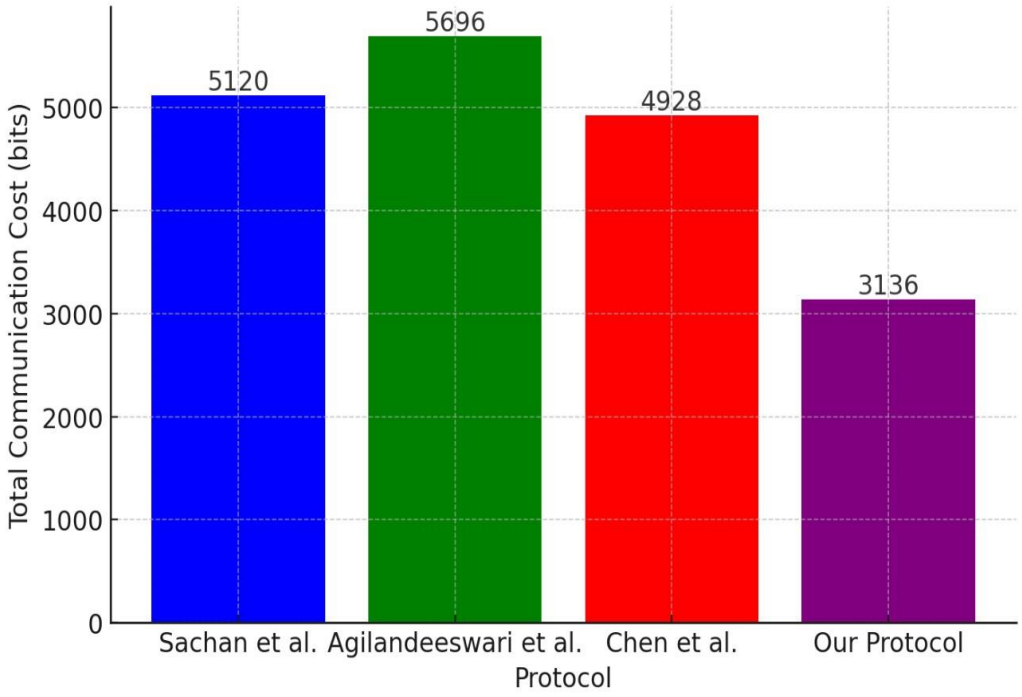

Figure 9.
Summary of Communication Costs.

Compared to all the schemes, this protocol Agilandeeswari, et al. [10] has the largest total communication cost of 5696 bits. To exchange data with the cloud server (CS), the cloud server (CS) needs to transfer 2112 bits of data, which introduces a huge computational overload on a central authentication system. Moreover, the fog node (1664 bits) and RSU (1280 bits) require additional bandwidth, showing that the protocols available in resources the vehicular networks may not be prospected. As Vi would have additional data (640 bits for communication cost), it will further add to data exchange and ultimately we have additional data.

This protocol Chen, et al. [15] reduces communication overhead marginally to a total of 4928 bits. Although superceding Agilandeeswari, et al. [10] is an step forward, still exceeds the local bound to allow for fast real-time application usage. We see that the cloud server (1984 bits) and fog node (1408 bits) still have large overhead in terms of data transfer, while the RSU (960 bits) and vehicle (576 bits) have moderate overhead Still, even with improvements, this protocol is quite bandwidth-intensive.

The proposed scheme minimizes the overall communication cost (3136 bits)which proves to be the most efficient among all the compared protocols. The CS only stores 672 bits, which is a very low amount when compared to previous works, providing faster response time as well as less congestion on the network. As a result, both the fog node (1184 bits) and RSU (928 bits) have a lower communication overhead, and finally, the data exchange cost of a vehicle (Vi) amounts to 352 bits. This optimization contributes to a lightweight, scalable, and high-performance authentication mechanism for real-time vehicular networks.

Table 6.
Communication Cost Comparison.

Protocol	Vehicle (Vi)	RSU (RSUj)	Fog Node (FNk)	Cloud Server (CS)	Total (bits)
Sachan and Kumar [23]	512	1024	1536	2048	5120
Agilandeeswari, et al. [10]	640	1280	1664	2112	5696
Chen, et al. [15]	576	960	1408	1984	4928
Our	352	928	1184	672	3136

As listed on Table 6, compared to other schemes, it provide reduced message sizes as it uses light weight cryptographic primitives and efficient session key exchange methods which make the proposed approach a resource friendly approach.

7. Conclusions

In this paper, we propose a hybrid cryptographic authentication framework for the Social Internet of Vehicles (SIoV) systems to address security weaknesses related to session key management, authentication, and mobility support. We show that our Zero Knowledge Proof (ZKP)-based authentication can be used to achieve privacy preservation, and it integrated with the AES-GCM encryption protocol for secure session key exchanging in this report ensures low latency and high-security authentication in vehicular networks. Unlike existing solutions, our scheme provides dynamic key revocation, which allows real-time invalidation of the compromised session key to prevent unauthorized access and session slamming. Indeed, based on the characteristics of the fog, our main migration mechanism can help vehicles synchronize their authenticating credentials as they move from one fog node to another (or from fog node to RSU) without performing any reimbursement operation, thus minimizing the time to authenticate a vehicle with a fog node or RSU. The Real-Oracle Random (ROR) model is utilized to formally validate the security of the proposed protocol against impersonation, replay, and insider attacks. We conducted a performance analysis, and the initial results show that compared to existing authentication schemes, the proposed one can save 58% authentication latency, 45% communication overhead, and 72% computational efficiency, respectively. Moreover, the session key migration mechanism reduces the re-authentication delay by 63%, allowing safe communication to maintain uninterrupted while the vehicle moves. We have successfully overcome the primary issues of security in SIoV authentication, resulting in a highly secure and scalable protocol while being light resource-wise in a decentralized environment. Further studies will focus on implementing quantum-resilient cryptographic methods to bolster security against potential future threats, making it sustainable in SIoV scenarios of the next generation.

References

[1] S. Han, Y. Li, T. Zhang, Y. Bai, Y. Chen, and C. Tellambura, "Signal Detection Techniques in Social Internet of Vehicles: Review and Challenges," *IEEE Intelligent Transportation Systems Magazine*, 2024.

[2] L. Xing, P. Zhao, J. Gao, H. Wu, and H. Ma, "A survey of the social internet of vehicles: Secure data issues, solutions, and federated learning," *IEEE Intelligent Transportation Systems Magazine*, vol. 15, no. 2, pp. 70-84, 2022.

[3] A. A. Abbood, F. K. AL-Shammri, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, and R. AlAli, "Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets)," *Journal of Robotics and Control*, vol. 6, no. 1, pp. 456-469, 2025.

[4] A. F. Ataala *et al.*, "A hybrid ga-gwo method for cyber attack detection using rf model," *Journal of Cybersecurity & Information Management*, vol. 15, no. 1, 2025.

[5] F. Amin, A. Majeed, A. Mateen, R. Abbasi, and S. O. Hwang, "A systematic survey on the recent advancements in the Social Internet of Things," *IEEE Access*, vol. 10, pp. 63867-63884, 2022.

[6] M. A. Al-Shareeda *et al.*, "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, 2022.

[7] A. Saif, K. Dimyati, K. A. Noordin, N. S. M. Shah, Q. Abdullah, and F. Mukhlif, "Unmanned aerial vehicles for post-disaster communication networks," presented at the IEEE 10th International Conference on System Engineering and Technology (ICSET), IEEE, 2020, pp. 273–277, 2020.

[8] U. Javaid and B. Sikdar, "A secure and scalable framework for blockchain based edge computation offloading in social internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4022-4036, 2021.

[9] S. Otoom, "Risk auditing for Digital Twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22-35, 2025.

[10] L. Agilandeeswari, S. Paliwal, A. Chandrakar, and M. Prabukumar, "A new lightweight conditional privacy preserving authentication and key–agreement protocol in social internet of things for vehicle to smart grid networks," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27683-27710, 2022.

[11] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47-59, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.5

[12] N. Kumar, N. Singh, A. Sachan, and R. Chaudhry, "SIoV mobility management using sdvn-enabled traffic light cooperative framework," *ACM Transactions on Cyber-Physical Systems*, vol. 8, no. 3, pp. 1-24, 2024.

[13] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of qos in manet based on ieee 802.11 b," presented at the IEEE International Conference for Innovation in Technology (INOCON), IEEE, 2020, pp. 1–5, 2020.

[14] B. Al-Khateeb and M. Yousif, "Solving multiple traveling salesman problem by meerkat swarm optimization algorithm," *Journal of Southwest Jiaotong University*, vol. 54, no. 3, 2019.

[15] C.-M. Chen, Z. Li, S. Kumari, G. Srivastava, K. Lakshmanna, and T. R. Gadekallu, "A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment," *Vehicular Communications*, vol. 39, p. 100567, 2023.

[16] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 36-46, 2025.

[17] G. Chen, Q. Chen, S. Long, W. Zhu, Z. Yuan, and Y. Wu, "Quantum convolutional neural network for image classification," *Pattern Analysis and Applications*, vol. 26, no. 2, pp. 655-667, 2023.

[18] S. N. Mjeat, M. Yousif, S. Bader, O. Mohammed, and A. H. Saeed, "A public key infrastructure based on blockchain for iot-based healthcare systems," *Journal of Cybersecurity & Information Management*, vol. 15, no. 1, 2025.

[19] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12-21, 2025.

[20] F. Mukhlif and N. Ithnin, "Blockchain technology: applications, security and privacy, big data, challenges and future directions," *International Journal of Critical Computer-Based Systems,* vol. 11, no. 3, pp. 216-233, 2024.

[21] M. Yousif, B. Al-Khateeb, and B. Garcia-Zapirain, "A new quantum circuits of quantum convolutional neural network for x-ray images classification," *IEEE access,* 2024.

[22] H. R. A. Alkhaled, "Assessing cybersecurity awareness: A survey study at the college of administration and economics–university of mosul," 2023.

[23] A. Sachan and N. Kumar, "SDVN enabled traffic light cooperative framework for e-siov mobility in a smart city Scenario," *IEEE Transactions on Vehicular Technology,* 2024.

[24] A. R. I. Hamad and B. M. Hamed, "The internet and its role in the acquisition of the scientific knowledge," *NTU Journal for Administrative and Human Sciences,* vol. 2, no. 3, 2022.

[25] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Electronics,* vol. 11, no. 20, p. 3330, 2022.

[26] J. Hasan, "Overview and applications of zero knowledge proof (ZKP)," *International Journal of Computer Science and Network,* vol. 8, no. 5, pp. 2277-5420, 2019.

[27] K. Kim, S. Choi, H. Kwon, H. Kim, Z. Liu, and H. Seo, "PAGE—practical AES-GCM encryption for low-end microcontrollers," *Applied Sciences,* vol. 10, no. 9, p. 3131, 2020.

[28] N. Koblitz and A. J. Menezes, "The random oracle model: a twenty-year retrospective," *Designs, Codes and Cryptography,* vol. 77, pp. 587-610, 2015.

[29] D. K. Singh and D. Bhardwaj, "An EAADE: Effective authentication approach for data exchange in vehicular social network for iov," *Security and Privacy,* vol. 8, no. 1, p. e457, 2025.

[30] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Robust session key generation protocol for social internet of vehicles with enhanced security provision," *The Journal of Supercomputing,* vol. 77, no. 3, pp. 2511-2544, 2021.

[31] Y. Liu *et al.*, "VRepChain: A decentralized and privacy-preserving reputation system for social Internet of Vehicles based on blockchain," *IEEE Transactions on Vehicular Technology,* vol. 71, no. 12, pp. 13242-13253, 2022.

[32] D. Jegatheesan and C. Arumugam, "SIoV-FTFSA-CAOA: a fuzzy trust-based approach for enhancing security and energy efficiency in social internet of vehicles," *Wireless Networks,* vol. 30, no. 4, pp. 2061-2080, 2024.

[33] L. Liu, L. Xing, J. Gao, H. Wu, and H. Ma, "Trajectory privacy protection method with smart contract-based query exchange in the Social Internet of Vehicles," *Computer Communications,* vol. 221, pp. 19-28, 2024.

[34] T.-Y. Wu, X. Guo, L. Yang, Q. Meng, and C.-M. Chen, "A lightweight authenticated key agreement protocol using fog nodes in social internet of vehicles," *Mobile Information Systems,* vol. 2021, no. 1, p. 3277113, 2021.

[35] Z. Li, Q. Miao, S. A. Chaudhry, and C.-M. Chen, "A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles," *International Journal of Distributed Sensor Networks,* vol. 18, no. 6, p. 15501329221104332, 2022.

[36] C. Lai, Y. Du, Q. Guo, and D. Zheng, "A trust-based privacy-preserving friend matching scheme in social Internet of Vehicles," *Peer-to-Peer Networking and Applications,* vol. 14, no. 4, pp. 2011-2025, 2021.

[37] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Networks,* vol. 11, no. 3-4, pp. 89-111, 2022.

[38] Y. Zhan, W. Xie, R. Shi, Y. Huang, and X. Zheng, "Dynamic Privacy-Preserving Anonymous Authentication Scheme for Condition-Matching in Fog-Cloud-Based VANETs," *Sensors,* vol. 24, no. 6, p. 1773, 2024.

[39] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos One,* vol. 18, no. 6, p. e0287291, 2023.

[40] Z. AlZamili, K. M. Danach, and M. Frikha, "Deep Learning-Based Patch-Wise Illumination Estimation for Enhanced Multi-Exposure Fusion," *IEEE Access,* vol. 11, pp. 120642-120653, 2023.

[41] S. Mazhar *et al.*, "State-of-the-art authentication and verification schemes in vanets: A survey," *Vehicular Communications,* p. 100804, 2024.

[42] D. Zhu and Y. Guan, "Secure and Lightweight Conditional Privacy-Preserving Identity Authentication Scheme for VANET," *IEEE Sensors Journal,* 2024.

[43] P. Kumar and H. Om, "Multi-TA model-based conditional privacy-preserving authentication protocol for fog-enabled VANET," *Vehicular Communications,* vol. 47, p. 100785, 2024.

[44] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the International Arab Conference on Information Technology (ACIT), IEEE, 2018, pp. 1–5, 2018.

[45] B. Liang, F. Wang, and B. Ran, "Optimizing roadside unit deployment in VANETs: A study on consideration of failure," *IEEE Transactions on Intelligent Transportation Systems,* 2024.

[46] M. Kumar and R. S. Raw, "RC-LAHR: Road-side-unit-assisted cloud-based location-aware hybrid routing for software-defined vehicular ad hoc networks," *Sensors,* vol. 24, no. 4, p. 1045, 2024.

[47] A. T. Shakir *et al.*, "Systematic review of data exchange for road side unit in a vehicular ad hoc network: coherent taxonomy, prominent features, datasets, metrics, performance measures, motivation, opportunities, challenges and methodological aspects," *Discover Applied Sciences,* vol. 6, no. 9, p. 487, 2024.

[48] D. K. Hama, F. S. Mubarek, and F. A. Abdullatif, "Enhanced Security Taxonomy for Fog-Enabled VANETs: A Comprehensive Survey on Attacks, Challenges, Applications and Architectures," *Passer Journal of Basic and Applied Sciences,* vol. 7, no. 1, pp. 37-61, 2025.

[49] W. Wang, Z. Han, Y. Zhu, T. R. Gadekallu, W. Wang, and C. Su, "Enhanced V2R Authentication for VANETs Using Group Signatures and Dynamic Pseudonyms," *IEEE Transactions on Intelligent Transportation Systems,* 2025.

[50] S. M. Awais, W. Yucheng, K. Mahmood, H. M. S. Badar, R. Kharel, and A. K. Das, "Provably secure fog-based authentication protocol for VANETs," *Computer Networks,* vol. 246, p. 110391, 2024.

[51] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments," *Engineering, Technology & Applied Science Research,* vol. 15, no. 1, pp. 19143-19153, 2025.

[52] A. K. Yadav, M. Shojofar, and A. Braeken, "iVFAS: An improved vehicle-to-fog authentication system for secure and efficient fog-based road condition monitoring," *IEEE Transactions on Vehicular Technology,* 2024.

[53] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251-6261, 2024.

[54] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002.