B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs

Sanjeev Kumar Dwivedi, *Student Member, IEEE*, Ruhul Amin, *Senior Member, IEEE*, Satyanarayana Vollala, *Member, IEEE*, and Muhammad Khurram Khan, *Senior Member, IEEE*

***Abstract*—The traditional handover authentication protocols in Vehicular Ad-hoc Network (VANET) suffer from important issues like single source of trust, Single-Point-of-Failure (SPoF), and fails to provide robust authentication due to several potential threats. In state-of-the-art of handover authentication, it takes high computation and communication overhead. The main aim of this paper is to integrate blockchain technology into the VANET system and to design a robust handover authentication protocol to solve the above-mentioned challenges. In this article, we design blockchain-based mutual authentication and session key agreement protocols for intra-vehicular and inter-vehicular (handover case) scenarios by implementing the hash function and Elliptic Curve Cryptography (ECC). We also validate the proposed model by using the Scyther tool and Real-Or-Random (ROR) oracle, standard model. The proposed scheme confirms security against all applicable attacks during security analysis. Furthermore, a detailed comparative analysis reveals that the proposed method has low communication and computation overheads and achieves more functionality features and security attributes than the relevant schemes.**

***Index Terms*—Blockchain, ECC, handover authentication, mutual authentication and session-key agreement, ROR model, VANET security.**

I. Introduction

WITH the rapid development and integration of innovative technologies (such as the Internet of Things (IoT), edge computing, and blockchain), various new intelligent applications have emerged to make people's lives easier. One of the most emerging fields is the Smart Transportation System (STS). In recent years, the STS has been a prominent study area for both industry and academia. Vehicular Ad-hoc Network (VANET) is the most popular network model for STS [1]. Vehicles in the STS collect information from their surroundings and disseminate it to other vehicles and roadside infrastructure (for instance, Road Side Unit (RSU)) through the On-Board Unit (OBU). Vehicle-to-vehicle (V2V) and vehicle-to-roadside unit (V2R) communication are established in VANET for exchanging information. Afterward, RSU sends data to the remote centralized Trusted Authority (TA) for further analysis, processing, and storage requirements.

Most of the VANET-recommended authenticated and key agreement security protocols have a centralized server architecture. The vehicles are generally required to register in the TA and authenticate with the fixed roadside infrastructure [2]. Moreover, in those systems, the TA is responsible for the registration, key distribution, certificate generation, and revocation of vehicles and RSU. Since TA is centralized, these systems are prone to various internal and external threats and suffer from the Single-Point-of-Failure (SPoF) problem [3]. However, the decentralization, mobility, non-trustworthiness, and security of V2V and V2R communication in the VANET system pose challenges in secure message dissemination and execution. Furthermore, in this system, when the vehicles move from one vehicular region to another region (or) one RSU coverage area to the next RSU, the vehicles need to register again with the TA and re-authenticate with the RSU of the foreign region. As a result, performing the foreign-domain authentication requires more processing and storage resources from the vehicle. As a result, we conclude that the solutions based on the centralized architecture are incompatible with the practical applications of the STS. The usage of blockchain in VANET can address these existing challenges.

Blockchain integrates cryptography, smart contracts, consensus mechanism, and distributed data storage (e.g., Interplanetary File System (IPFS)) to provide immutable [4] and traceable records. The characteristics of blockchain ensure data auditability, and nodes are held accountable for their operations. As a result, it achieves data security and offers the inherent trust for blockchain-enabled applications [5]. Over the last few years, researchers have investigated the applicability of blockchain in the STS. They primarily embraced the blockchain for secure message dissemination, access control, and managing the key pairs of vehicular nodes. However, the optimum solution for the handover authentication of vehicles is at the initial stage only and is still considered an open challenge. To resolve this issue, we

Manuscript received 5 September 2022; revised 17 February 2023; accepted 23 March 2023. Date of publication 24 April 2023; date of current version 25 October 2023. This work was supported by the International Institute of Information Technology Naya Raipur (IIIT-NR), Chhattisgarh, India. The work of Muhammad Khurram Khan was supported by King Saud University, Riyadh, Saudi Arabia under Project RSP2023R12. Recommended for acceptance by Dr. Dejun Yang. *(Corresponding author: Muhammad Khurram Khan.)*

Sanjeev Kumar Dwivedi, Ruhul Amin, and Satyanarayana Vollala are with the Department of Computer Science and Engineering (CSE), Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, (IIIT-NR), Chhattisgarh 493661, India (e-mail: sanjeevdwivedi131988@gmail.com; amin_ruhul@live.com; satya4nitt@gmail.com).

Muhammad Khurram Khan is with the King Saud University, Riyadh 11653, Saudi Arabia (e-mail: mkhurram@ksu.edu.sa).

Digital Object Identifier 10.1109/TNSE.2023.3264829

2327-4697 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

propose a blockchain-based handover authentication protocol to have secure communication in the VANET.

A. Research Contributions

The contributions of the paper present the following points:

- This article presents the blockchain-based mutual authentication and session key agreement protocol by utilizing the Elliptic Curve Cryptography (ECC) and one-way hash function (1) between the vehicle and RSU of the same region (intra-vehicular domain), (2) between the vehicle and RSU of two different regions (inter-vehicular domain), (3) between the RSU of two different vehicular domains.
- The proposed system consists of two blockchains: Auxiliary blockchain and parent blockchain. The edge RSU of every vehicular network maintains an auxiliary blockchain, whereas all base RSU and RA maintain a parent blockchain.
- We then perform the informal and formal security analysis of the proposed scheme by using the widely accepted Real-Or-Random (ROR) oracle model and Scyther tool that finally proves that the proposed scheme can persist against the various known attacks.
- This paper also provides a comprehensive comparison of computation and communication overheads, and the proposed system's fundamental security and functioning features with state-of-the-art research in VANET. The results show that the proposed scheme has superior security and low communication and computation overheads.

B. Organization of the Paper

This article is organized as follows: Section I provides the introductory information about our paper, including the main contributions. The related works for the blockchain-based access control and handover authentication schemes utilized in the VANET system are presented in Section II. Section III exhibits the system and threat models of the proposed system. Section IV offers the proposed solution and the various phases of our model, such as mutual authentication and session key for both intra-vehicular and inter-vehicular domains. The detailed informal and formal security analysis of the proposed system based on the Scyther and ROR model is elaborated in Section V. Section VI presents the performance of our model and comparative analysis with the state-of-the-art protocols. Section VII presents the concluding remarks and the future scope of this paper.

II. Related Works

In this Section, our research team covers the existing state-of-the-art works utilizing blockchain technology in the VANET system.

A. Blockchain-Based Privacy Preserving and Authentication Schemes

The authentication and privacy of the vehicles are essential aspects in the STS. An adversary can take advantage in launching internal and external attacks if these security aspects are not provided in the underlying VANET. To incorporate this, the research community tries to develop a blockchain-based solution that should support vehicle privacy and its authentication very securely and efficiently. Lu et al. [6] proposed a blockchain-enabled privacy-preserving authentication scheme where the vehicle's certificates and its real identity are stored in the blockchain that finally provides transparency among the semi-trusted authorities. The extended version of the merkle patricia tree-based structure performs the distributed authentication of the sender. To address the automatic realization of user registration and its public key revocation, a smart contract-enabled decentralized key management approach was proposed by Ma et al. [7]. The bivariate polynomial function-based session key provides mutual authentication between vehicles and RSU. In order to provide secure communication in ITS, blockchain-enabled certificate-based authentication protocol is designed by Vangala et al. [8]. In this protocol, the edge server participates in the consensus process and creates a partial block for the associated transaction, whereas the cloud server does the complete block creation. Furthermore, Chattaraj et al. [9] designed a blockchain-based certificateless key agreement protocol for the smart transportation system. The voting-based consensus mechanism verifies the block, and the cloud servers maintain the peer-to-peer blockchain network. To achieve accuracy in the transmitted message, Feng et al. [10] proposed a blockchain-assisted $BPAS$ protocol where the system automatically performs the vehicle's authentication and preserves the vehicle's privacy. The smart contract is written in JavaScript programming and implemented in the hyperledger fabric platform. Zhao et al. [11] proposed a blockchain-assisted privacy-preserving announcement protocol by employing the identity-based group signature scheme to achieve the vehicle's anonymity. RSU uses the weighted sum method to evaluate the vehicle's reputation, and a joint Proof-of-Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) consensus mechanism are adopted for block verification.

B. Blockchain-Based Handover Authentication Schemes

In the STS, vehicles frequently migrate from one vehicular domain to another, and due to this movement, the network imposes extra computation and communication overhead on the vehicles. Recently, researchers utilized the blockchain mechanism to solve the problems that occurred during the migration of vehicles and suggested the handover authentication protocols in the VANET-based system. Wang et al. [12] proposed a blockchain-assisted scalable computation scheme to achieve the handover authentication of vehicles through the secure ownership transfer mechanism. Here, blockchain records the vehicle's attribute, trust level, and its confidence level to execute the V2I handover Authentication. In [13], the authors proposed the blockchain-based anonymous handover authentication scheme for the VANET application. In this system, whenever the vehicle joins the new coverage area of RSU, the system utilizes the blockchain to conduct the bilinear pairing-enabled vehicle authentication. Sharma et al. [14] proposed a blockchain-based secure mist computing network model by leveraging the

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

TABLE I
CONTEMPORARY WORKS IN THE BLOCKCHAIN-ENABLED SMART TRANSPORTATION SYSTEM

Works	Problem Statement	Proposed Solution	Cryptographic Features	Limitations
Vangala *et al.* [8]	Vehicle accident detection and notification in STS	Blockchain-enabled certificate-based authentication protocol	Utilized one-way hash function, symmetric encryption, and decryption, ECC	Does not support handover authentication and foreign region of vehicles communication
Chattaraj *et al.* [9]	Certificate-based key agreement protocol requires the trusted authority to issue the certificates	Blockchain-enabled certificateless key agreement protocol	Utilized one-way hash function, Bivariate polynomial, ECDSA	Does not support handover authentication and node accountability
Feng *et al.* [10]	Credibility and trustworthiness of transmitted messages	Blockchain-based privacy-preserving and authentication protocol	Utilized fuzzy extractor, attribute-based encryption, ECC, one-way hash function	Requires high computational cost and does not support handover authentication
Zhao *et al.* [11]	Focus on the privacy of announcement messages	Blockchain-assisted and identity-based group signature protocol	Utilized bilinear pairings, ECC, one-way hash functions, and symmetric encryption	Does not support handover authentication and V2V communication at foreign region
Wang *et al.* [12]	Rapid re-authentication of vehicles when it joins the new coverage area of RSU	Blockchain-assisted scalable handover authentication protocol	Utilized bilinear pairings, one-way hash functions	Does not support blockchain security simulation solution
Maria *et al.* [13]	Reduce the computational overhead in the vehicle's re-authentication process	Blockchain-enabled exchanging of secure authentication code protocol	Utilized bilinear pairings, ECC, one-way hash functions	Does not support foreign region of vehicles communication and blockchain security simulation solution
Sharma *et al.* [14]	Focus on the latency, availability, and scalability issues in the smart transportation system	Blockchain-enabled secure mist computing network model	Utilized aggregate signature scheme, PUF symmetric key, hash function	Does not support handover authentication and session key negotiation protocol.
Yu *et al.* [18]	Reduces the redundant frequency of vehicles experienced in handover authentication	Blockchain and ECC-based handover authentication scheme in the 5G wireless networks	Utilized different hash functions, ECC	Does not support mutual authentication and untraceability properties
Li *et al.* [19]	Focus on the low handover authentication efficiency of the vehicle access authentication in IoV	Blockchain-assisted pre-authentication and handover authentication scheme with low communication overhead	Utilized one-way hash function, asymmetric encryption, and decryption, signature generation and verification	Does not investigate the computation of the session key and the mechanism behind the authenticity of the target RSU

computing resources at the edge of the network. This system employs an aggregated signature method that can enhance the privacy of devices. Furthermore, the smart contract deployed at the edge of the network performs the authentication of devices. The authors introduced the blockchain-based handover authentication mechanism for the wireless network in [15]. A multi-attribute authority's attribute-based signature technique with a constant size is utilized, to provide secure handover authentication in the wireless network and address the SPoF problem experienced by the central system. Similarly, Wang et al. [16] presented the handover authentication for intelligent tele-health based on the blockchain mechanism in the multi-server edge computing environment. The authenticated edge server assists the handover authentication, and it does the execution of the required operations. As a consequence, the system's processing overhead is reduced.

Recently, Son et al. [17] suggested a pairing-free handover authentication scheme for VANET based on the blockchain. This model supports Real-Or-Random (ROR) oracle standard model and Burrows–Abadi–Needham (BAN) logic. Similarly, Yu et al. [18] utilized a blockchain solution in the 5 G wireless networks to achieve the handover authentication during the V2R communication. This scheme reduces the redundant frequency of vehicles experienced during their handover authentication. This scheme records the information of vehicles in the blockchain, and then the smart contracts validate it during the handover of vehicles. But, this scheme does not guarantee mutual authentication and untraceability properties and is prone to physical vehicle capture attacks. A blockchain-assisted pre-authentication and handover authentication scheme for the Internet-of-Vehicles (IoV) is suggested by the authors in [19]. This scheme focuses on increasing the efficiency and decreasing the computation overhead of the system that occurred because of the handover of the vehicles. However, the authors do not investigate and analyze the session key negotiation between the end entities. Feng et al. [20] developed a cross-domain authentication scheme for the intelligent internet of drones using the blockchain. They designed multiple signatures-assisted threshold sharing and smart contracts to achieve drones' domain joining and authentication. Further, the authors used bilinear mapping for the signature and domain verification of drones. A brief summary of a few existing privacy-preserving and authentication schemes, along with their cryptographic features and limitations, is presented in Table I.

With the closer investigation of Sections II-A and II-B, we have found that a minimal number of researchers have considered the blockchain-empowered handover authentication of the vehicles in the VANET system. The suggested schemes that incorporate the handover mechanism suffer from high overheads and do not support multi-vehicular domain authentication of vehicles. Moreover, these schemes are not suitable for large vehicular networks.

The various notations which are used throughout the protocol are presented in Table II.

III. SYSTEM MODEL

In this Section, we discuss the network and threat models, which are very necessary to build our proposed protocol.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

TABLE II
NOTATIONS AND ITS MEANING

Symbol	Description
DID^k	Identity of k^{th} vehicular domain
RA^k	Registration authority of k^{th} vehicular domain
rsu_i^k	i^{th} RSU of k^{th} vehicular domain
veh_j^k	j^{th} vehicle of k^{th} vehicular domain
$ID_{rsu_i^k}$	Identity of rsu_i^k
$SI_{rsu_i^k}$	Secret information of rsu_i^k
$(PUB_{rsu_i^k}, PRI_{rsu_i^k})$	Public and private key pair of rsu_i^k
(PUB_{RA^k}, PRI_{RA^k})	Public and private key pair of RA^k
$SSK_{rsu^k-RA^k}$	Shared session key between rsu^k and RA^k
$BI_{rsu_i^k}$	Registration block for rsu_i^k
$ID_{veh_j^k}$	Identity of veh_j^k
$SI_{veh_j^k}$	Secret information of veh_j^k
T_j	Current time-stamp for vehicle registration
$P_{veh_j^k}$	New value created using the hashing of $ID_{veh_j^k}$, $SI_{veh_j^k}$, and T_j
$PIN_{veh_j^k}$	PIN number of veh_j^k
$PID_{veh_j^k}$	Pseudo-identity of veh_j^k
$BI_{veh_j^k}$	Registration block for veh_j^k
$mer_{veh_j^k}$	Merkle-root value corresponding to $BI_{veh_j^k}$
n_j	Nonce selected for the creation of new block corresponding to $BI_{veh_j^k}$
$(r_j, v_j, u_j, b_i, c_m)$	Random numbers
$h(\cdot)$	One-way hash function (256-bit)
G	An additive group G of elliptic curve points with order q
P	Generator (or) base point of G
$k \cdot P$	Elliptic curve scalar multiplication which is $P + P + ... + P$ (k-times)
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation operator

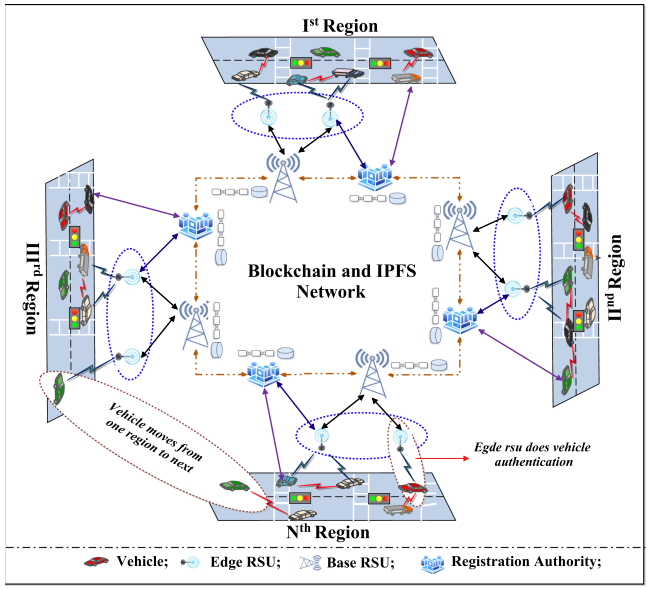

Fig. 1. Systematic architecture of proposed scheme.

A. Network Model

In this subsection, a detailed description of the proposed system model is presented. As shown in Fig. 1, the entire VANET system is divided into multiple vehicular regions, and each vehicular region consists of four entities: Registration Authority (RA), Edge RSU and Base RSU, Vehicles, Blockchain with IPFS.

Registration Authority (RA): The RA of each vehicular region publishes the system's public parameters and deploys RSU in its region. The RA performs the registration of vehicles and RSU (both edge RSU and base RSU) and creates a new block for each registration based on the blockchain mechanism, which is termed a registration block. The registration block for RSU and vehicle is created based on the $\langle ID_{rsu_i}, PUB_{rsu_i} \rangle$, and $\langle ID_{veh_j}, P_{veh_j} \rangle$ respectively.

Roadside Unit (RSU): In each vehicular domain, two types of RSU are present: edge RSU and base RSU. The edge RSU has less computation and storage capability than the base RSU. The edge RSU performs the authentication of vehicles before communication, which further depends on the intra-vehicular or inter-vehicular domains. In the intra-vehicular situation, the edge RSU authenticates the vehicle from its vehicular domain, whereas in the inter-vehicular case, the edge RSU first communicates with the edge RSU of other vehicular-domain, and then the authentication of the vehicle is performed by the system.

The base RSUs have more storage capacity, and they, along with the RA, maintain the parent blockchain. Reducing network latency is the primary notion behind introducing the two types of RSU. The RA deploys the fixed number of base RSUs and performs the registration. Once the registration procedure is successfully executed, the base RSU joins the parent blockchain network and becomes part of it.

Vehicles: The vehicles are equipped with the OBU, and they have very less computation and storage capability. Every vehicle is registered with the respective RA of the vehicular domain. The vehicle sends crucial messages (for instance, traffic jam, accident, etc.) to its nearby edge RSU. The edge RSU authenticates the vehicle by using blockchain and then considers the message as trustworthy message.

Blockchain and IPFS: The proposed system maintains two levels of blockchain: auxiliary blockchain and parent blockchain. The edge RSU of every vehicular region maintains its own auxiliary blockchain, whereas the base RSU and RA of all vehicular domains maintain the parent blockchain. After RA registers the vehicles, it uploads the $\langle ID_{veh_j}, P_{veh_j} \rangle$ to auxiliary blockchain. Then the edge RSU of the corresponding vehicular domain verifies whether a vehicle has registered (or not) and performs the authentication of vehicles with the help of an auxiliary blockchain. Once the V2R authentication process has finished, the edge RSU performs the digital signature on messages (using a scheme such as ECDSA), performs encryption on it using a public key, and then transmits the ciphered message to the base RSU. The base RSU first deciphers the received message and then stores it in the IPFS. The IPFS returns a hash value in its response, which is finally stored in the parent blockchain. The characteristics of blockchain ensures that the data uploaded on auxiliary and parent blockchains can not be modified (or forged). Moreover, storing the message on the IPFS also reduces the storage cost of the blockchain network.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

Smart Contracts: These are computerized scripts, unlike traditional paper-based contracts, that are carried out automatically once the requirements of the pre-programmed contracts between the peers (nodes) are met. They run on a distributed system, like the Ethereum blockchain. Therefore, a trusted third party is not needed to carry out the transactions (or validate the assets). By leveraging Ethereum-empowered smart contracts, our suggested approach safely records the registration information of both vehicles and RSU, and also retrieves it whenever necessary. By doing this, the immutable registration information is stored in the blockchain network.

B. Threat Model

This Section covers the threat model, which is associated with our proposed blockchain-assisted handover authentication protocol. We have used broadly accepted "Canetti-Krawczyk (CK) [21]" threat models to evaluate the security strength of our proposed protocol. The threat model is a formalization of the adversary, and according to this formalization, the adversary can be programmed about its abilities and intentions. The goal of the adversary is to acquire unauthorized access to the system and then to try to be benefited from it. In our proposed threat model, we also assume that the adversary has the requisite software. The capabilities of the adversary are as follows:

- The adversary has enough capability to intercept the public messages communicated between veh_j^k and rsu_i^k and it can inject the false messages and delete and modify the exchanged messages. However, the messages which are transmitted securely cannot be intercepted by the adversary.
- The adversary can compromise the OBU of the vehicle and then extract the sensitive parameters stored on it using the power-analysis attacks [22]. Once the adversary gets the vehicle's sensitive parameters and public messages, it may attempt to launch well-known security attacks such as impersonation attacks, insider attacks, and man-in-the-middle attacks.
- Moreover, the adversary can compromise the secret credentials with the session keys or the session states in particular sessions. However, if the present session key has been revealed in the specific session, the adversary cannot guess the past and future session keys.
- It is impossible for the adversary to guess the real identity of the vehicle even if entities of the proposed system collide.
- In last, it is our valid assumption that it is very likely for the adversary to guess one secret information at a time. But, it is computationally infeasible for an adversary to guess the two pieces of secret information in polynomial time.

IV. Proposed System

This Section presents the proposed blockchain-based mutual authentication and session-key agreement protocol for V2R communication, which is further divided into two possible scenarios. Under the first scenario, the edge RSU authenticates the vehicle for the same domain (i.e., Intra-vehicular domain), whereas, in the second scenario, the edge RSU authenticates the vehicle of the foreign domain (i.e., Inter-vehicular domain). In addition, this Section also presents the mutual authentication protocol between two edge RSUs of two different vehicular domains. A detailed description of various phases is provided in the following Subsections.

A. System Initialization Phase

With the mutual consensus among all RAs of vehicular domains, the RA of k^{th} vehicular domain (i.e., RA^k) chooses two large prime numbers p and q, and an additive elliptic cyclic group G with order q. RA^k then chooses a generator P of G, and a random number $s \in Z_q^*$ as a private key PRI_{RA^k} and finally computes the corresponding public key $PUB_{RA^k} = s \cdot P. RA^k$ further computes the shared session key $SSK_{rsu^k - RA^k}$ for all RSUs $SSK_{rsu^k - RA^k} = h(DID^k \parallel ID_{rsu^k} \parallel PRI_{RA^k})$, and transmits it to the corresponding RSU through a secure channel. RA^k also selects the one-way cryptographic secure hash function $h(\cdot)$.

B. Registration Phase

1) Roadside Unit (RSU) Registration: Before deploying RSUs in the vehicular network, each RSU must perform its registration through the registration authority of its domain. Here, we assume that the RA of k^{th} region is RA^k and RA^k performs the registration of all RSU belonging to k^{th} region. To make the registration procedure more clear, this phase considers the registration of i^{th} RSU belonging to k^{th} region, i.e., rsu_i^k.

Step-1: Initially rsu_i^k selects its unique identity $ID_{rsu_i^k}$ and secret information $SI_{rsu_i^k}$, and then securely sends parameters $\langle ID_{rsu_i^k}, SI_{rsu_i^k} \rangle$ to RA^k.

Step-2: Once RA^k gets $\langle ID_{rsu_i^k}, SI_{rsu_i^k} \rangle$, it utilizes the smart contracts and computes the key-pair of rsu_i^k as $PRI_{rsu_i^k} = h(SI_{rsu_i^k} \parallel SSK_{rsu_i^k - RA^k})$; $PUB_{rsu_i^k} = PRI_{rsu_i^k} \cdot P$, where $PRI_{rsu_i^k} \in Z_q^*$.

Step-3: After the computation of $\langle PUB_{rsu_i^k}, PRI_{rsu_i^k} \rangle$, RA^k creates a registration-block $BI_{rsu_i^k}$ by considering the $\langle ID_{rsu_i^k}, PUB_{rsu_i^k} \rangle$ as transaction parameters, and then adds the registration-block of rsu_i^k into the parent blockchain.

Step-4: If Step-3 is successfully executed, RA^k utilizes the secret channel and then sends the index of the registration-block along with the key-pair $\langle PUB_{rsu_i^k}, PRI_{rsu_i^k}, BI_{rsu_i^k} \rangle$ to rsu_i^k.

Step-5: rsu_i^k further computes $W_i = BI_{rsu_i^k} \oplus h(SI_{rsu_i^k})$, and very securely stores $\langle SI_{rsu_i^k}, W_i, PRI_{rsu_i^k}, DID^k \rangle$ in its memory and publicly announces the $\langle PUB_{rsu_i^k}, ID_{rsu_i^k} \rangle$.

2) Vehicle Registration: If any vehicle wants to take (or provide) services from our system, it must have to register in our system. The registration procedure for j^{th} vehicle of k^{th} region (i.e., veh_j^k) through the RA^k is as follows.

Step-1: Initially veh_j^k chooses its unique identity $ID_{veh_j^k}$, secret information $SI_{veh_j^k}$, PIN number $PIN_{veh_j^k}$, and then very securely sends parameters $\langle ID_{veh_j^k}, SI_{veh_j^k} \rangle$ to RA^k. The $PIN_{veh_j^k}$ is used to activate the OBU.

Step-2: Once RA^k receives $\langle ID_{veh_j^k}, SI_{veh_j^k} \rangle$, it computes $P_{veh_j^k} = h(ID_{veh_j^k} \parallel SI_{veh_j^k} \parallel T_j)$ through the

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

pre-programmed code written in the smart contracts. Here, T_j refers to the current time-stamp used for vehicle registration.

Step-3: Now, RA^k computes a registration-block $BI_{veh_j^k}$ for veh_j^k by referring $\langle ID_{veh_j^k}, P_{veh_j^k} \rangle$ as transaction parameters, and then includes the $BI_{veh_j^k}$ into the auxiliary blockchain.

Step-4: If Step-3 is successfully executed, RA^k further computes the pseudo-identity $PID_{veh_j^k}$ for veh_j^k as $PID_{veh_j^k} = h(mer_{veh_j^k} \parallel BI_{veh_j^k}) \oplus n_j$, where $mer_{veh_j^k} = h(h(ID_{veh_j^k}) \parallel h(P_{veh_j^k}))$, and uses the secret channel for sending the parameters $\langle PID_{veh_j^k}, BI_{veh_j^k} \rangle$ to veh_j^k.

Step-5: veh_j^k selects a random number r_j, computes $A_j = h(ID_{veh_j^k} \parallel PIN_{veh_j^k}) \oplus r_j$, $Q_j = BI_{veh_j^k} \oplus h(r_j)$, $R_j = h(PID_{veh_j^k} \parallel BI_{veh_j^k} \parallel Q_j)$, and then stores the parameters $\langle PID_{veh_j^k}, A_j, Q_j, R_j, DID^k \rangle$ in vehicles OBU, and finally drops $BI_{veh_j^k}$.

Each RA repeats the same procedure for the registration of every RSU and vehicle in its vehicular domain.

C. Vehicle User Login Phase

After the successful registration of vehicles, whenever a vehicle wants to provide any crucial message (which it has collected from its surrounding environment), the vehicle's OBU first checks whether the vehicle user is a legitimate person or not. This checking is necessary because it may be possible that the attacker physically captured the vehicle and then tried to send the messages. The step-wise procedure for the login of the vehicle's user is as follows.

Step-1: The vehicle's user enters $ID^*_{veh_j^k}$ and $PIN^*_{veh_j^k}$. The OBU of vehicle computes $r_j^* = h(ID^*_{veh_j^k} \parallel PIN^*_{veh_j^k}) \oplus A_j$, $BI^*_{veh_j^k} = Q_j \oplus h(r_j^*)$, and $R_j^* = h(PID_{veh_j^k} \parallel BI^*_{veh_j^k} \parallel Q_j)$.

Step-2: Now, OBU verifies if $(R_j^* = R_j)$. If this condition is correct, OBU predicts that the vehicle's user is the correct person and temporarily stores the $BI^*_{veh_j^k}$, which is further useful in mutual authentication and session-key agreement phase (See Section IV-D).

D. Blockchain-Based Mutual Authentication and Session-Key Agreement Phase Between Vehicle and Edge RSU

This Section describes the proposed mutual authentication followed by the session-key agreement protocol between the vehicle and edge RSU. After the successful execution of the vehicle login phase, the vehicle may send the collected crucial messages to the nearby edge RSU. But, before considering the message as trustworthy, both vehicle and edge RSU first mutually approve each other and then establish the session key for secure communication on both sides.

1) Case 1: For Intra-Vehicular Domain: Here, we consider that the j^{th} vehicle of k^{th} vehicular domain (i.e., veh_j^k) sends the messages to i^{th} RSU of same k^{th} vehicular domain (i.e., rsu_i^k).

Step-1: Initially, veh_j^k chooses a random secret $v_j \in Z_q^*$, and computes two random points as $X = v_j \cdot PUB_{rsu_i^k} = (X_x, X_y)$, and $Y = v_j \cdot P$. Further, veh_j^k computes $M_0 = DID^k \oplus ID_{rsu_i^k}$, $M_1 = h(DID^k \parallel X_x \parallel T_1)$, $M_2 = PID_{veh_j^k} \oplus M_1$, $M_3 = h(PID_{veh_j^k} \parallel ID_{rsu_i^k} \parallel X \parallel T_1)$, $M_4 = h(PID_{veh_j^k} \parallel X_y \parallel T_1) \oplus BI^*_{veh_j^k}$, and then sends parameters $\langle M_0, M_2, M_3, M_4, Y, T_1 \rangle$ to rsu_i^k through the public channel. Here T_1 is the present time-stamp.

Step-2: After getting $\langle M_0, M_2, M_3, M_4, Y, T_1 \rangle$, rsu_i^k checks the validity of T_1. If it is correct, rsu_i^k further computes $X^* = Y \cdot PRI_{rsu_i^k} = (X_x^*, X_y^*)$, $DID^{k^*} = M_0 \oplus ID_{rsu_i^k}$, $M_1^* = h(DID^{k^*} \parallel X_x^* \parallel T_1)$, $PID^*_{veh_j^k} = M_2 \oplus M_1^*$, $M_3^* = h(PID^*_{veh_j^k} \parallel ID_{rsu_i^k} \parallel X^* \parallel T_1)$, and verifies the condition $(M_3^* = M_3)$. If $(M_3^* = M_3)$ is not satisfied, rsu_i^k aborts the operation. Otherwise $BI^{**}_{veh_j^k} = h(PID^*_{veh_j^k} \parallel X_y^* \parallel T_1) \oplus M_4$.

Step-3: By computing the DID^{k^*}, rsu_i^k knows that in which vehicular-domain veh_j^k has registered, and accordingly rsu_i^k continues for mutual authentication procedure (i.e., authentication for intra-vehicular domain or inter-vehicular domain). Once rsu_i^k has recomputed the $BI^{**}_{veh_j^k}$, it retrospects the auxiliary blockchain and checks the existence of $BI^{**}_{veh_j^k}$ in the blockchain. If it is available, rsu_i^k fetches $ID_{veh_j^k}$ corresponding to the $BI^{**}_{veh_j^k}$, and declares the veh_j^k as an authentic vehicle.

Step-4: If Step-3 has successfully executed, rsu_i^k chooses a random secret $b_i \in Z_q^*$, and computes two random points as $Z_1 = b_i \cdot Y$, and $Z_2 = b_i \cdot P$. rsu_i^k further computes $M_5 = h(ID_{veh_j^k} \parallel Z_1 \parallel T_2)$, $SK_{ij} = h(Z_1 \parallel BI^{**}_{veh_j^k})$, $VERI_{SK_{ij}} = h(SK_{ij} \parallel X_x^*)$, and sends the parameters $\langle Z_2, M_5, VERI_{SK_{ij}}, T_2 \rangle$ to veh_j^k via the public channel. Here T_2 is the present time-stamp.

Step-5: After getting $\langle Z_2, M_5, VERI_{SK_{ij}}, T_2 \rangle$, veh_j^k checks the validity of T_2. If it is valid, veh_j^k further computes $Z_1^* = v_j \cdot Z_2$, $M_5^* = h(ID_{veh_j^k} \parallel Z_1^* \parallel T_2)$, and verifies the condition $(M_5^* = M_5)$. If $(M_5^* = M_5)$ is correct, rsu_i^k is authenticated by veh_j^k. Step-1 to Step-5 ensures that both veh_j^k and rsu_i^k mutually authenticated each other.

Step-6: veh_j^k further computes $SK_{ij} = h(Z_1^* \parallel BI^*_{veh_j^k})$, and $VERI^*_{SK_{ij}} = h(SK_{ij} \parallel X_x)$. If $(VERI^*_{SK_{ij}} = VERI_{SK_{ij}})$, then the verification of session key is successful. Once SK_{ij} has established between veh_j^k and rsu_i^k, they can use SK_{ij} for exchanging the messages.

2) Case 2: For Inter-Vehicular Domain: Here, we consider that the j^{th} vehicle of k^{th} vehicular domain (i.e., veh_j^k) sends the messages to m^{th} RSU of n^{th} vehicular domain (i.e., rsu_m^n. This means that in *Case 2*, rsu_m^n considers veh_j^k as foreign vehicle.

Step-1: Initially, veh_j^k chooses a random secret $u_j \in Z_q^*$, and computes two random points as $A = u_j \cdot PUB_{rsu_m^n} = (A_x, A_y)$, and $B = u_j \cdot P$. Further, veh_j^k computes $M_{00} = DID^k \oplus ID_{rsu_m^n}$, $M_{11} = h(DID^k \parallel A_x \parallel T_3)$, $M_{22} = PID_{veh_j^k} \oplus M_{11}$, $M_{33} = h(PID_{veh_j^k} \parallel ID_{rsu_m^n} \parallel A \parallel T_3)$, $M_{44} = h(PID_{veh_j^k} \parallel A_y \parallel T_3) \oplus BI^*_{veh_j^k}$, and then sends

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

parameters $\langle M_{00}, M_{22}, M_{33}, M_{44}, B, T_3\rangle$ to rsu_m^n through the public channel, where T_3 is the current time-stamp, and veh_j^k has obtained $BI^*_{veh_j^k}$ in login phase (See Subsection IV-C).

Step-2: After getting $\langle M_{00}, M_{22}, M_{33}, M_{44}, B, T_3\rangle$, rsu_m^n checks the validity of T_3. If it is correct, rsu_m^n further computes $A^* = B \cdot PRI_{rsu_m^n} = (A_x^*, A_y^*)$, $DID^{k*} = M_{00} \oplus ID_{rsu_m^n}$, $M_{11}^* = h(DID^{k*} \parallel A_x^* \parallel T_3)$, $PID^*_{veh_j^k} = M_{22} \oplus M_{11}^*$, $M_{33}^* = h(PID^*_{veh_j^k} \parallel ID_{rsu_m^n} \parallel A^* \parallel T_3)$, and verifies the condition $(M_{33}^* = M_{33})$. If $(M_{33}^* = M_{33})$ is not satisfied, rsu_m^n aborts the operation. Otherwise rsu_m^n computes $BI^{**}_{veh_j^k} = h(PID^*_{veh_j^k} \parallel A_y^* \parallel T_3) \oplus M_{44}$.

Step-3: By computing the DID^{k*}, rsu_m^n knows that veh_j^k has registered in k^{th} vehicular-domain, and the information corresponding to $BI^{**}_{veh_j^k}$ is not available in the auxiliary registration blockchain, maintained by the edge RSU of n^{th} vehicular-domain. Therefore, in order to perform the authentication of veh_j^k, rsu_m^n contacts with any RSU of k^{th} vehicular-domain. The RSU of k^{th} vehicular-domain does the aforementioned task and provides its acknowledgment message to the rsu_m^n, which confirms that veh_j^k is an authentic vehicle. The Section IV-E clearly explains how two edge RSUs of different domains communicate with each other and share the authentication information of veh_j^k.

Step-4: If Step-3 has successfully executed, rsu_m^n chooses a random secret $c_m \in Z_q^*$, and computes two random points as $Z_{11} = c_m \cdot B$, and $Z_{22} = c_m \cdot P$. rsu_m^n further computes $M_{55} = h(ID_{veh_j^k} \parallel Z_{11} \parallel T_4)$, $SK_{mj} = h(Z_{11} \parallel BI^{**}_{veh_j^k})$, $VERI_{SK_{mj}} = h(SK_{mj} \parallel A_x^*)$, and sends the parameters $\langle Z_{22}, M_{55}, VERI_{SK_{mj}}, T_4\rangle$ to veh_j^k via the public channel. Here T_4 is the present time-stamp.

Step-5: After getting $\langle Z_{22}, M_{55}, VERI_{SK_{mj}}, T_4\rangle$, veh_j^k checks the validity of T_4. If it is valid, veh_j^k further computes $Z_{11}^* = u_j \cdot Z_{22}$, $M_{55}^* = h(ID_{veh_j^k} \parallel Z_{11}^* \parallel T_4)$, and verifies the condition $(M_{55}^* = M_{55})$. If $(M_{55}^* = M_{55})$ is correct, rsu_m^n is authenticated by veh_j^k. Step-1 to Step-5 ensures that both veh_j^k and rsu_m^n mutually authenticated each other.

Step-6: veh_j^k further computes $SK_{mj} = h(Z_{11}^* \parallel BI^*_{veh_j^k})$, and $VERI^*_{SK_{mj}} = h(SK_{mj} \parallel A_x)$. If $(VERI^*_{SK_{mj}} = VERI_{SK_{mj}})$, then the verification of session key is successful. Once SK_{mj} has established between veh_j^k and rsu_m^n, they can use SK_{mj} for exchanging the messages.

E. Blockchain-Based Mutual Authentication and Session-Key Agreement Phase Between Edge RSUs of Two Different Vehicular-Domains

Here, we consider that the m^{th} RSU of n^{th} vehicular-domain rsu_m^n wants to exchange the information of veh_j^k from i^{th} RSU of k^{th} vehicular-domain rsu_i^k. The step-wise procedure for communication between rsu_m^n and rsu_i^k is as follows.

Step-1: Initially, rsu_m^n provides $SI_{rsu_m^n}$ and computes $BI_{rsu_m^n} = W_m \oplus h(SI_{rsu_m^n})$. After getting $BI_{rsu_m^n}$, rsu_m^n chooses a random secret $e_m \in Z_q^*$, and computes two random points as $E = e_m \cdot PUB_{rsu_i^k} = (E_x, E_y)$, and $F = e_m \cdot P$. Further, rsu_m^n computes $R_1 = h(ID_{rsu_i^k} \parallel E_x \parallel T_5)$, $R_2 = R_1 \oplus BI_{rsu_m^n}$, and sends $\langle R_2, F, T_5\rangle$ to rsu_i^k through the public channel. Here T_5 is the present time-stamp.

Step-2: After receiving $\langle R_2, F, T_5\rangle$, rsu_i^k computes $E^* = F \cdot PRI_{rsu_i^k} = (E_x^*, E_y^*)$, $R_1^* = h(ID_{rsu_i^k} \parallel E_x^* \parallel T_5)$, and $BI_{rsu_m^n} = R_1^* \oplus R_2$. In the proposed system, base RSU and RA maintain the registration block for every edge RSU (i.e., in the parent blockchain). Therefore, in order to get the information of $BI_{rsu_m^n}$, rsu_i^k encrypts $BI_{rsu_m^n}$ using $SSK_{rsu_i^k - RA^k}$. The RA^k decrypts it using $SSK_{rsu_i^k - RA^k}$, retrospects the blockchain and checks the existence of $BI_{rsu_m^n}$ in the blockchain. If it is available, RA^k declares that rsu_m^n is an authentic node and sends the positive acknowledgment to rsu_i^k, which is encrypted using the same $SSK_{rsu_i^k - RA^k}$.

Step-3: If Step-2 has successfully executed, rsu_i^k chooses a random secret $g_i \in Z_q^*$, and and computes two random points as $G = g_i \cdot F = (G_x, G_y)$, and $H = g_i \cdot P$. Further, rsu_i^k computes $R_3 = h(R_1^* \parallel G_x \parallel T_6)$, $R_4 = R_3 \oplus BI_{rsu_i^k}$, $SK_{mi}^{rsu} = h(G \parallel 111)$, and $VERI_{SK_{mi}^{rsu}} = h(SK_{mi}^{rsu} \parallel E_y^*)$, and sends $\langle H, R_4, VERI_{SK_{mi}^{rsu}}, T_6\rangle$ to rsu_m^n through the public channel, where T_6 is the current time-stamp.

Step-4: After getting $\langle H, R_4, VERI_{SK_{mi}^{rsu}}, T_6\rangle$, rsu_m^n checks the validity of T_6. If it is correct, rsu_m^n further computes $G^* = e_m \cdot H = (G_x^*, G_y^*)$, $R_3^* = h(R_1 \parallel G_x^* \parallel T_6)$, and $BI_{rsu_i^k} = R_3^* \oplus R_4$. Now, in order to authenticate the rsu_i^k, rsu_m^n continues with the same procedure as mentioned in Step-2. The only difference is that this time $SSK_{rsu_m^n - RA^n}$ key is used for communication between rsu_m^n and RA^n.

Step-5: Once RA^n confirms that rsu_i^k is an authentic node, rsu_m^n computes $SK_{mi}^{rsu} = h(G^* \parallel 111)$, and $VERI^*_{SK_{mi}^{rsu}} = h(SK_{mi}^{rsu} \parallel E_y)$. If $(VERI^*_{SK_{mi}^{rsu}} = VERI_{SK_{mi}^{rsu}})$, then the verification of session key is successful. Once SK_{mi}^{rsu} has established between rsu_i^k and rsu_m^n, they can use SK_{mi}^{rsu} for exchanging the messages. For instance, rsu_m^n encrypts $BI^{**}_{veh_j^k}$ by using established the key SK_{mi}^{rsu} and sends the encrypted message to rsu_i^k. On the other side, rsu_i^k decrypts it using the SK_{mi}^{rsu}, retrospects the blockchain for the existence of $BI^{**}_{veh_j^k}$, and then finally based on the availability, confirms to the rsu_m^n.

F. Data Storage & Accessing Phase

The data storage and accessing phase begins once the vehicle and edge RSU mutually authenticate each other and establish a session key. Once the session key has been established, the vehicle can use the session key for secure sharing of data (e.g., traffic jam information, accidents) to edge RSU. We assume that veh_j^k and rsu_i^k are mutually authenticated with each other and negotiated a session key SK_{ij} (as presented in Section IV-D). veh_j^k sends the data using SK_{ij} to rsu_i^k. Once rsu_i^k gets the data, it forwards the same to the base RSU. After that, base RSU utilizes the IPFS and parent blockchain to store the data and returned hash, respectively. Here, the heavy volume of the data is stored on the IPFS, whereas the parent blockchain stores the

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

hash returned by the IPFS. As a result, the utilization of IPFS in the proposed system minimizes the storage overhead on the blockchain. The end-user (e.g., traffic authority) can access the data from IPFS if it gets the hash value stored on the blockchain. In paper [1], our research team deeply elaborated on "how the hashes are exchanged among the peer blockchain nodes through the access control mechanism."

V. Security Analysis and Verification

In this Section, the security analysis and verification of the proposed protocol using informal and formal models are presented. The various propositions are incorporated to support the informal analysis, which finally strengthens our proposed model.

A. Informal Security Analysis of Known Attacks

Proposition 1: The proposed protocol is secure against the replay attack.

Proof: In our proposed protocol, every message transmitted over the public channel has a unique time-stamp (for instance, $\langle M_0, M_2, M_3, M_4, Y, T_1\rangle$), which is verified at the receiver side before accepting the public messages. Therefore, the presence of a time-stamp in every public message prevents vehicles and RSU from transmitting the same messages. Thus, the proposed protocol is resilient against the replay attack.

Proposition 2: The proposed protocol is secure against the man-in-the-middle attack.

Proof: In our proposed protocol, the message-hashes $\langle M_3, M_4, M_5, M_{33}, M_{44}, M_{55}\rangle$ are sent over the public channel. Due to pre-image resistance characteristics of hash functions, an adversary A cannot obtain the real values of these hashed messages. Moreover, A cannot get the secret values stored in the messages $\langle Z_2, Z_{22}, F, H\rangle$ because of ECDLP assumption. Thus, this informal analysis concludes that the proposed scheme is resilient against the man-in-the-middle attack.

Proposition 3: The proposed protocol is robust against the privileged-insider attack.

Proof: Assuming that adversary A obtains $\langle ID_{veh_j^k}\rangle$ during the registration of veh_j^k. However, A cannot compute the $P_{veh_j^k}$ because it cannot get PRI_{RA^k}. Moreover, if A gets PRI_{RA^k} by some means, it cannot compute $PID_{veh_j^k} = h(mer_{veh_j^k} \parallel BI_{veh_j^k}) \oplus n_j$, because it is very difficult to guess two unknown parameters $\langle BI_{veh_j^k}, n_j\rangle$. Therefore, A cannot establish SK_{ij} without knowing the $BI_{veh_j^k}$. Hence, we conclude that our proposed protocol is secured against the privileged-insider attack.

Proposition 4: The proposed protocol is safe against the impersonation attack.

Proof: Suppose A eavesdrops messages $\langle M_0, M_2, M_3, M_4, Y, T_1\rangle$ through the open channel and tries to behave as legitimate veh_j^k, where $M_0 = DID^k \oplus ID_{rsu_i^k}$, $M_1 = h(DID^k \parallel X_x \parallel T_1)$, $M_2 = PID_{veh_j^k} \oplus M_1$, $M_3 = h(PID_{veh_j^k} \parallel ID_{rsu_i^k} \parallel X \parallel T_1)$, $M_4 = h(PID_{veh_j^k} \parallel X_y \parallel T_1) \oplus BI^*_{veh_j^k}$. In order to generate the fake messages, A picks a random number v'_j, and computes $X' = v'_j \cdot PUB_{rsu_i^k} = (X'_x, X'_y)$. However, without the knowledge of valid $BI^*_{veh_j^k}$, A cannot compute M_4. The $BI^*_{veh_j^k}$ is used by the rsu_i^k for authentication of veh_j^k. Hence, the proposed scheme is robust against the impersonation attack.

Proposition 5: The proposed protocol is secure against the physical vehicle capture attack.

Proof: In this attack, A utilizes the power analysis attacks [23] for extracting the stored parameters $\langle PID_{veh_j^k}, A_j, Q_j, R_j, DID^k\rangle$ from the OBU of the compromised veh_j^k. However, without the knowledge of $PIN_{veh_j^k}$, r_j, $BI_{veh_j^k}$, A cannot compute valid (A_j, Q_j, R_j). Moreover, all the loaded parameters in OBU of veh_j^k are distinct from non-compromised vehicles, and it is not helpful for establishing the session key among the respective edge RSUs. Therefore, the proposed protocol is secured against the physical vehicle capture attack.

Proposition 6: The proposed protocol is safe against the session key disclosure attack.

Proof: The protection of session key $SK_{ij} = h(Z_1 \parallel BI_{veh_j^k})$ depends on two secret numbers (b_i, v_j) and $BI_{veh_j^k}$. The proposed protocol has not shared $\langle b_i, v_j, BI_{veh_j^k}\rangle$ over the open channel. Moreover, it is infeasible for A to extract Z_1 and (b_i, v_j) due to the difficulty of inversion of the cryptographic one-way hash function and hardness of ECDLP. Therefore, the valid SK_{ij} cannot be computed by A.

Proposition 7: The proposed scheme is robust against the sybil attack.

Proof: In the proposed protocol, veh_j^k provides its identity $ID_{veh_j^k}$ to RA^k. The RA^k identifies whether $PID_{veh_j^k}$ corresponding to $ID_{veh_j^k}$ is available or not in its memory. If available, then RA^k predicts that veh_j^k has registered in our system, and $BI_{veh_j^k}$ is available in the blockchain. As a result, RA^k does not issue $PID_{veh_j^k}$ and declares that veh_j^k has already registered. Therefore, the probability of getting multiple identities is negligible. Hence, we conclude that the proposed scheme is secure against the sybil attack.

Proposition 8: The proposed scheme provides mutual authentication.

Proof: In our proposed protocol, rsu_i^k and rsu_m^n obtains $\langle PID_{veh_j^k}, BI_{veh_j^k}\rangle$ during the authentication phase from veh_j^k. However, these parameters are not shared in the plain-text format through the public channel. The rsu_i^k (or rsu_m^n) retrieves the hash of $\langle ID_{veh_j^k}, P_{veh_j^k}\rangle$ from the blockchain to authenticate veh_j^k, which are unknown to other vehicles and RSU. Furthermore, veh_j^k retrieves Z_1 (or Z_{11}) through the public channel, which is used to authenticate rsu_i^k (or rsu_m^n), respectively, according to its vehicular domains. The *Proposition 6* claims that adversary A cannot forge the Z_1 (or Z_{11}). Therefore, the proposed scheme attains mutual authentication.

Proposition 9: The proposed protocol exhibits known key secrecy.

Proof: Assuming by some means, the present session key SK_{ij} is disclosed to A. A then tries to compute the previous and future session keys. SK_{ij} has been computed by using the secret values v_j and b_i, which is modified in every session. The mathematical equation for computing $SK_{ij} = h(Z_1 \parallel BI_{veh_j^k})$

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

where $Z_1 = b_i \cdot Y$ and $Y = v_j \cdot P$. Therefore, A cannot construct previous and future session keys if SK_{ij} is disclosed. Hence, the proposed scheme validates known key secrecy.

Proposition 10: The proposed protocol is secure against the ephemeral secret leakage (ESL) attack.

Proof: In the intra-vehicular domain authentication phase, veh_j^k and rsu_i^k negotiate a session key $SK_{ij} = h(Z_1 \parallel BI_{veh_j^k})$ for secure communication; whereas, in the inter-vehicular domain authentication phase, veh_j^k and rsu_m^n negotiate a session key $SK_{mj} = h(Z_{11} \parallel BI_{veh_j^k})$ for their secret communication. The computation of $\langle SK_{ij}, SK_{mj} \rangle$ are based on the long-term secrets ($BI_{veh_j^k}$) and session-specific ephemeral secrets (Z_1, Z_{11}). Furthermore, the computation of Z_1 and Z_{11} is depends on the random numbers; where $Z_1 = b_i \cdot Y$; $Y = v_j \cdot P$ and $Z_{11} = c_m \cdot B$; $B = u_j \cdot P$. Since, the SK_{ij} and SK_{mj} utilizes the random secrets $\langle b_i, v_j, c_m, u_j \rangle$, which is changed in every session. As a result, the proposed protocol always creates a different session key. Thus, if the session key of a specific session has been revealed, it will not affect other sessions. Therefore, we conclude that the proposed protocol provides perfect forward and backward secrecy and is robust against the ESL attack.

Proposition 11: The proposed scheme provides vehicle anonymity and untraceability.

Proof: To conduct vehicle authentication, the proposed scheme uses $PID_{veh_j^k}$; as a result, $ID_{veh_j^k}$ is not unveiled in both intra-vehicular and inter-vehicular scenarios for vehicle authentication. Furthermore, A cannot obtain $PID_{veh_j^k}$ from the public messages $\langle M_0, M_2, M_3, M_4 \rangle$ and $\langle M_{00}, M_{22}, M_{33}, M_{44} \rangle$. As a result, A cannot trace veh_j^k during the authentication phase. Therefore, the proposed scheme guarantees the vehicle anonymity and untraceability property.

B. Formal Security Verification Under Scyther Tool

Before deploying the security protocols in real networks, it is necessary to examine the strength of the security provided by the protocols. To achieve it, the proposed protocol is simulated by using the Scyther simulator, which formally proves that the protocol is secure from all types of possible attacks. Scyther has recently gained prominence in checking and analyzing security protocols, and it is noted for its enhanced features and excellent performance [24]. Figs. 2 and 3 demonstrate the communication process between vehicles and RSU, and between two RSUs are secure, and the secret parameters are not revealed during their communication. The suggested protocol is simulated several times in various environments, and each simulation shows that there are no attacks within the specified bounds. The simulation finding reveals that the noninjective agreement (Ni-Agree) and noninjective synchronization (Ni-Synch) are met. The Ni-Agree asserts that the communication parties agree on variable values that are transferred between them, and the results of the analysis confirm that this assertion is accurate. The Ni-Synch property necessitates the execution of the relevant sending and receiving events by the runs specified by the cast function, and it is implemented in the proper sequence.

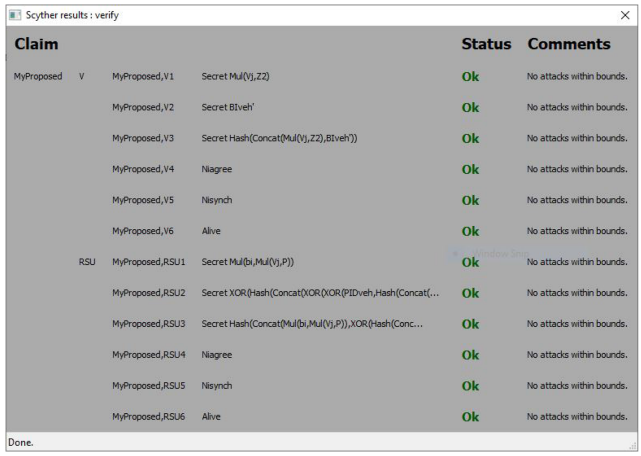

Fig. 2. Scyther output for communication between vehicle and roadside unit.

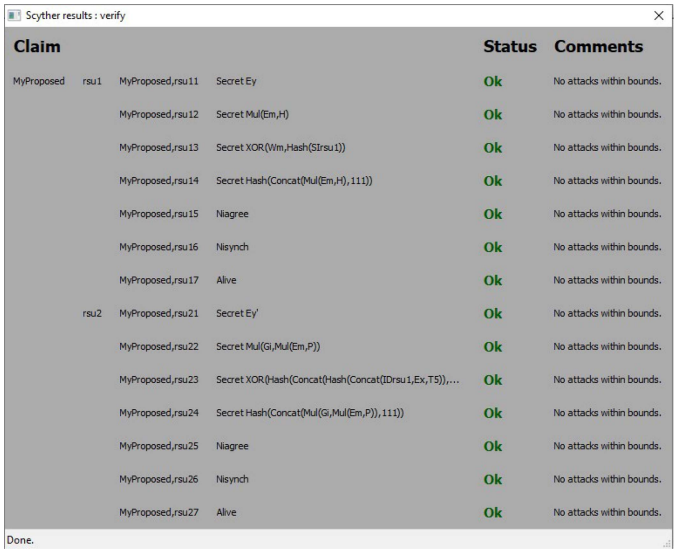

Fig. 3. Scyther output for communication between vehicle two roadside units.

C. Formal Security Analysis Under ROR Model

This section indicates how effective our approach is at achieving the required security using Real-Or-Random (ROR) model [25]. Its most essential features are listed below.

Participants Vehicle (V_i), edge RSU (rsu_m), base RSU (RSU_n), and RA (RA_p) are the four participants in the proposed method. Each participant can operate multiple instances, and these instances are referred to as oracles. Let π^i, π^f, π^u, and π^c represent the V_i, rsu_m, RSU_n, and RA_p with instances i, f, u, and c respectively. We sometimes use π^n to represent instances of V_i, rsu_m, RSU_n, and RA_p.

Partnering When the following requirements are met simultaneously, the instances π^{n1} and π^{n2} are deemed partnered: (1) They have the same communication session-id $session_{id}$, and (2) all messages they send and receive are distinct.

Freshness If the session key SK formed between π^{n1} and π^{n2} has not been leaked to an attacker A, the instances π^{n1} and π^{n2} are deemed fresh.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

Adversary The adversary A has complete control over the communication channel, including the ability to listen, manipulate, invent, and insert messages. Querying oracles is used to replicate the adversary's ability. The following queries are available to A.

Execute(π^i, π^f, π^u, π^c): This query is conducted by an A to obtain all messages sent between members V_i, rsu_m, RSU_n, and RA_p during the protocol execution. This query simulates an adversary's passive attack.

Send(π^n, m): A sends the participant instance π^n a message m, and π^n responds with a message once the $Send$ query is run. The purpose of this query is to imitate active attacks.

CorruptUD(π^u): Physical vehicle capture attack is simulated using this query. This query can be used by an adversary A to extract data from OBU of the vehicle.

CorruptITD(π^u): The attack in which the vehicle is hijacked is modeled in this query. When this query is run, the hidden data in the vehicle is given to A.

ConstructSK(π^i, π^f, π^u, π^c): By intercepting messages, this query can be used to create the SK_{ij} between any two communicating entities.

CorruptUD and CorruptITD query satisfies the weak-corruption paradigm, as specified in [26], demonstrating that the participant instance's temporal keys and data have not been altered.

Test(π^n): Session key's semantic security is modeled using this query. To find the result of the *Test*, the query uses a randomly chosen concealed bit b. *Test* outputs the undefined symbol $Gamma$ if the instance π^n is unable to construct a session key before an adversary A runs the *Test* query. If the established session key of π^n is fresh, When $b = 1$, the *Test* query yields the authentic session key. When $b = 0$, it returns a random key of identical length. The objective of the A is to figure out the value of the concealed bit b used by this query. The attacker has sufficiently broken the session key's semantic security if A can consistently predict the value of the right b.

Random Oracle: The entities, including A, have access to the cryptographic hash function h(·) in our scheme. A random oracle is used to represent the h(·). Assume Hash is a random oracle query.

Semantic Security of Session Key: The adversary in the ROR model must be able to distinguish between a true session key and a random key of identical length. On the instance π^n, A can run several *Execute*, *Send*, *CorruptUD*, *CorruptITD*, *ConstructSK*, and *Test* queries. At the end of the game, A predicts that bit b using the *Test* will be b', if b' = b, A will win. Allow Suc to be an occurrence in which A wins the game. A's advantage in breaching the proposed scheme's session key semantic security S_1 is defined as $Adv_S^{SK1}(A) = |2 \cdot Pr[Suc_0] - 1|$. Under the ROR model, for any probabilistic polynomial time (PPT) adversary A, we assert that the suggested scheme S_1 is semantically safe if a negligible function ϵ exists, which fulfills $Adv_S^{SK1}(A) \leq \epsilon$.

Theorem 1: Suppose A is an adversary of PPT that compromises the session key's $(SK1)$ semantic security between vehicle and roadside unit in the ROR model, and S_1 be the proposed scheme between vehicle and RSU. Let q be the number of bits present in response R_k. A's advantage in compromising our scheme $S1$'s session key semantic security is predicted to be

$$Adv_S^{SK1}(A) \leq q_h^2/|H| + (2Adv_S^{IF}(A) \cdot q_{send1})/2^q$$

where q_h, q_{send1}, $|H|$, and Adv_S^{IF}(A) respectively signify the number of Hash queries, the number of Send queries for guessing R_k, the domain space of the hash function, and the benefits of recreating session key$(SK1)$.

Proof: We establish a sequence of games g_i (i = 0,1,2,3,4,5) and define Suc_i as the event in which A successfully guesses the concealed bit b in game g_i.

g_0*:* Under the ROR paradigm, the game mimics an attack by attacker A against the suggested scheme S_1. Because the attacker must guess b before the game. Then, we have

$$Adv_S^{SK1}(A) = |2 \cdot Pr[Suc_0] - 1| \tag{1}$$

g_1*:* An adversary A mimics an eavesdropping attempt on an open channel in this game. A can execute multiple *Execute*(π^i, π^f, π^u, π^c) queries. Then A is instructed to do a series of *Test*(π^n) queries. $\langle M_1, M_3, M_4 \rangle$ are the only messages that A can listen in on. A must compute $SK_{ij} = h(Z_1 \parallel BI_{veh_j^k})$ to get the session key. Because A is unaware of the parameters Z_1 and $BI_{veh_j^k}$, the chances of adversary A winning game g_1 remain unchanged. Consequently, we have

$$Pr[Suc_1] - Pr[Suc_0] = 0 \tag{2}$$

g_2*:* $Hash$ and $Send$ queries are modeled on g_1 in g_2. An active attack can be performed using g_2 in which the adversary attempts to fabricate a message in order to trick the other side into believing that it is an authentication message. A does this by trying to find if there is a hash collision by continually running the Hash query. To conduct the $Send$ query, there is no issue for the adversary A, because each exchanged message in our scheme comprises certain hidden parameters, the timestamp, and the nonce. According to the birthday paradox, we have

$$|Pr[Suc_2] - Pr[Suc_1]| \leq q_h^2/2|H| \tag{3}$$

g_3*:* By joining the simulations of the *CorruptITD* and *ConstructSK* queries, g_2 is turned into g_3. A can get the challenge Ck from vehicle with the help of *CorruptITD* query. The adversary must be able to guess b_i and thus compute the parameter $Z_1 = b_i \cdot Y$ so as to compute $SK_{ij} = h(Z_1 \parallel BI_{veh_j^k})$. where $BI_{veh_j^k}$ is obtained using the *ConstructSK* query and Z_1 is obtained via the *CorruptITD* query. Let $Adv_S^{IF}(A)$ be the adversary's advantage in reassembling the session key $(SK1)$. The likelihood of A correctly predicting $R_k \in \{0,1\}^q$ is about $1/2^q$.

$$|Pr[Suc_3] - Pr[Suc_2]| \leq Adv_S^{IF}(A) \cdot (q_{send1}/2^q) \tag{4}$$

Because all of the queries in g_3 are simulated, to win the game, A just needs to guess the secret bit b after performing the *Test* query. So, we have

$$Pr[Suc_3] = 1/2 \tag{5}$$

From (1)–(5), we get

$$Adv_S^{SK1}(A) \leq q_h^2/|H| + (2Adv_S^{IF}(A) \cdot q_{send1})/2^q$$

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

VI. Performance Analysis

This Section covers the communication and computational costs that occurred during the initial authentication and handover authentication of the proposed scheme. Furthermore, the presented solution's computed costs and security and functionality features are compared with state-of-the-art research.

A. Communication Cost

In order to calculate the communication cost, the value of time-stamp, identity, random numbers, and block index are considered 32-bit, 160-bit, 160-bit, and 256-bit. The size of elliptic curve point $P = (P_x, P_y)$ is 320-bit, where P_x and P_y are x and y coordinates of point P. The SHA-256 hashing technique has also been considered for $h(\cdot)$ computation, which yields a fixed 256-bit result.

Case 1: The communication cost incurred during the intra-vehicular scenario is depicted in case 1, where vehicles and edge RSU of the same vehicular domain communicate and establish a session key for sharing their data. During the initial authentication, two messages $\langle M_0, M_2, M_3, M_4, Y, T_1\rangle$ and $\langle Z_2, M_4, VERI_{SK_{ij}}, T_2\rangle$ are communicated between veh_j^k and rsu_i^k which demand (160 + 256 + 256 + 256 + 320 + 32) = 1280-bits and (320 + 256 + 256 + 32) = 864-bits respectively. Therefore, the total communication cost for sending these two messages is 2144-bits.

Case 2: The communication cost incurred during the inter-vehicular scenario is depicted in case 2, where vehicles and edge RSU of two different vehicular domains communicate and establish a session key for sharing their data. During the handover authentication, four messages $\langle M_{00}, M_{22}, M_{33}, M_{44}, B, T_3\rangle$, $\langle R_2, F, T_5\rangle$, $\langle H, R_4, VERI_{SK_{mi}^{rsu}}, T_6\rangle$ and $\langle Z_{22}, M_{44}, VERI_{SK_{mj}}, T_4\rangle$ are exchanged among veh_j^k, rsu_m^n and rsu_i^k which demand (160 + 256 + 256 + 256 + 320 + 32) = 1280-bits, (256 + 320 + 32) = 608-bits, (320 + 256 + 256 + 32) = 864-bits, and (320 + 256 + 256 + 32) = 864-bits, respectively. Therefore, the total communication cost for sending these four messages is 3616-bits.

The Son et al. [17] and Maria et al. schemes [13] demand for 2 × (256 + 256 + 320 + 32) = 2 × 864 = 1728-bits and (320 + 32 + 160) = 512-bits during the V2R initial authentication respectively whereas, these schemes require 2 × (256 + 256 + 320 + 32 + 256 + 256 + 256 + 32) = 2 × 1664 = 3328-bits and (320 + 320 + 320 + 320) = 1280-bits for V2R handover authentication respectively. However, this scheme does not support the multi-vehicular domain authentication of vehicles and does not suitable for the large vehicular network. In addition to it, in Maria et al. schemes [13], the messages HK_1 and HK_2 are sent over the public channel and integrity of these two messages are not verified at the side of current RSU. Therefore, this scheme does not achieve the confidentiality and handover integrity of public messages. In continuation of it, Wang et al. scheme [12] demands 1056-bits and 3072-bits during the initial and handover authentication, respectively. But, this scheme does not support the mutual authentication property and does not consider the privileged-insider attack scenario in its solution.

TABLE III
Comparative Study on Communication Costs

Scheme	BC/NBC	No. of messages exchanged	Total communication cost (in bits)
Wang *et al.* [12] (Initial authentication)	BC	1	1056
Wang *et al.* [12] (Handover authentication)	BC	3	3072
Maria *et al.* [13] (Initial authentication)	BC	1	512
Maria *et al.* [13] (Handover authentication)	BC	2	1280
Son *et al.* [17] (Initial authentication)	BC	2	1728
Son *et al.* [17] (Handover authentication)	BC	4	3328
Gao *et al.* [27] (Initial authentication)	NBC	3	6016
Gao *et al.* [27] (Pre-handover authentication)	NBC	3	7440
Gao *et al.* [27] (Handover authentication)	NBC	3	5984
Xu *et al.* [28] (Initial authentication)	NBC	6	6432
Xu *et al.* [28] (Handover authentication)	NBC	11	7584
Jiang *et al.* [29] (Initial authentication)	NBC	5	5536
Jiang *et al.* [29] (Handover authentication)	NBC	3	3008
Gao *et al.* [30] (Initial authentication)	NBC	4	2624
Gao *et al.* [30] (Handover authentication)	NBC	3	4160
Proposed Scheme (Initial authentication)	BC	2	2144
Proposed Scheme (Handover authentication)	BC	4	3616

BC: The scheme has adopted blockchain based security solution; NBC: The scheme has adopted non-blockchain based security solution.

Gao et al. scheme [27] requires the 6016-bits, 7440-bits, and 5984-bits for the initial authentication, pre-handover authentication, and handover authentication, respectively. The communication overhead of scheme mentioned in [28], [29] and [30] is (6432-bits, 7584-bits), (5536-bits, 3008-bits) and (2624-bits, 4160-bits), respectively for initial and handover authentication. However, all of these schemes do not incorporate blockchain technology in their solutions. The overall communication cost comparison of the proposed scheme with the relevant existing methods is presented in Table III, and the same is illustrated in Fig. 4. It is observed that the proposed scheme consumes an adequate number of bits in its communication and also achieves the multi-vehicular domain authentication of vehicles with the support of a blockchain mechanism.

B. Computation Cost

To calculate the computation cost of the proposed protocol and further compare it with the existing relevant schemes, our research team has used the results (approximated amount of time needed by the various cryptographic primitives) that have already been presented in [8], and [2]. In this research work, we represent T_{bp}, T_{ecm}, T_{eca}, T_{ex}, T_h, T_{mm}, and T_{mi} as the time

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

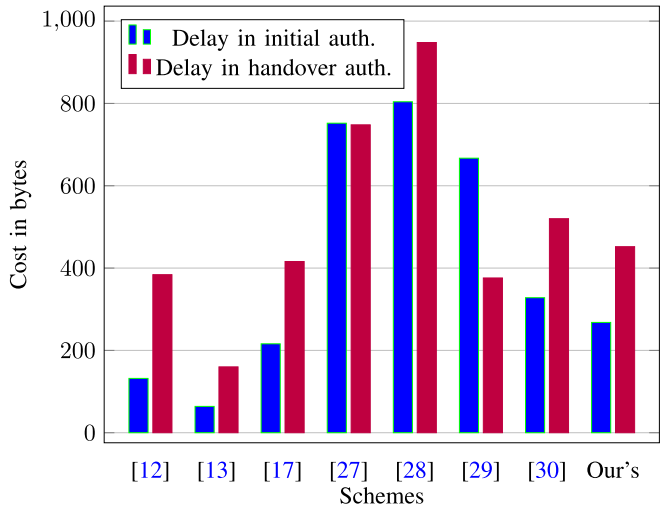

Fig. 4. Comparison of total communication cost.

TABLE IV
COMPARATIVE STUDY ON COMPUTATION COSTS

Scheme	BC/NBC	Initial authentication	Handover authentication
Wang *et al.* [12]	BC	$6T_{ex} + 3T_{mm} + 2T_{mi} + 4T_{bp} + 4T_h$	$6T_{ex} + 5T_{mm} + 2T_{bp} + 2T_h$
Maria *et al.* [13]	BC	$6T_{ex} + 2T_{ecm} + 2T_{bp} + 4T_h$	$7T_{ex} + 2T_{ecm} + 2T_{bp} + 3T_h$
Son *et al.* [17]	BC	$6T_{ecm} + 19T_h$	$9T_{ecm} + 28T_h + T_{eca}$
Xu *et al.* [28]	NBC	$17T_h + 10T_{ecm} + 3T_{se} + 3T_{sd} + 2T_{sg} + 2T_{sv}$	$23T_h + 15T_{ecm} + 3T_{se} + 3T_{sd} + 2T_{sg} + 2T_{sv}$
Jiang *et al.* [29]	NBC	$2T_{sg} + 2T_{sv} + 8T_{ecm} + 4T_{se} + 4T_{sd} + 3T_{mtp} + T_{gsg}$	$T_{sg} + T_{sv} + 7T_{ecm} + 2T_{se} + T_{sd} + 3T_{mtp} + T_{gsg} + T_{gsv}$
Proposed	BC	$6T_{ecm} + 12T_h$	$12T_{ecm} + 21T_h$

T_{se} : time required for symmetric encryption; T_{sd} : time required for symmetric decryption; T_{sg} : time required for generating the signature; T_{sv} : time required for verification of signature; T_{mtp} : time required by map-to-point hash function; T_{gsg} : time required for generating the group-signature; T_{gsv} : time required for verifying the group-signature; BC: The scheme has adopted blockchain-based security solution; NBC: The scheme has adopted non-blockchain based security solution.

taken by the bilinear pairing operation, elliptic curve scalar multiplication, elliptic curve point addition, exponentiation operation, one-way hash function, modular multiplication operation, and modular inverse operation, respectively. Then we have $T_{bp} \approx 42.11$ ms, $T_{ecm} \approx 17.10$ ms, $T_{eca} \approx 4.4$ ms, $T_{ex} \approx 19.20$ ms, $T_h \approx 0.32$ ms, $T_{mm} \approx 0.88$ ms, and $T_{mi} \approx 2.64$ ms.

Case 1: The computational cost incurred during the intra-vehicular scenario is depicted in case 1, where vehicles and edge RSU of the same vehicular domain communicate and establish a session key for sharing their data. In this case, the detailed discussion of the computation cost for the mutual authentication and session key agreement between vehicle veh_j^k and roadside unit rsu_i^k of the k^{th} vehicular domain is presented. veh_j^k and rsu_i^k both separately require three scalar point multiplication and six hash computation for generating and verifying the messages $\langle M_0, M_2, M_3, M_4 \rangle$ and for the computation of session key SK_{ij}. As a result, initial authentication requires the computation cost of $6T_{ecm} + 12T_h \approx 106.44$ ms.

Case 2: The computational cost incurred during the inter-vehicular scenario is depicted in case 2, where vehicles and edge RSU of the two different vehicular domains communicate and establish a session key for sharing their data. In this case, the detailed discussion of the computation cost for the mutual authentication and session key agreement between vehicle veh_j^k of the k^{th} vehicular domain and roadside unit rsu_m^n of the n^{th} vehicular domain is presented. The veh_j^k requires six hash and three scalar point multiplication operations, and rsu_i^k requires three scalar point multiplication and four hash computation. Whereas rsu_m^n requires eleven hash and six scalar point multiplication operations for generating the messages and for the computation of session key SK_{mj}. As a result, handover authentication requires the computation cost of $12T_{ecm} + 21T_h \approx 211.92$ ms.

The Son et al. [17] scheme requires $6T_{ecm} + 19T_h \approx 108.67$ ms of computation cost during the initial authentication whereas, for the handover authentication, it requires $9T_{ecm} + 28T_h + T_{eca} \approx 167.26$ ms of computation cost. Maria et al. [13] scheme utilizes bilinear pairing and ECC cryptosystem in their solution. The total computation cost of this scheme is $6T_{ex} + 2T_{ecm} + 2T_{bp} + 4T_h \approx 234.9$ ms for initial authentication and $7T_{ex} + 2T_{ecm} + 2T_{bp} + 3T_h \approx 253.78$ ms for handover authentication. This scheme requires high computation cost than the proposed one due to the involvement of bilinear pairing operation. Furthermore, the scheme presented in [12] needs $6T_{ex} + 3T_{mm} + 2T_{mi} + 4T_{bp} + 4T_h \approx 292.84$ ms and $6T_{ex} + 5T_{mm} + 2T_{bp} + 2T_h \approx 204.46$ ms for the initial and handover authentication respectively. Table IV presents the comparative analysis of the proposed scheme with the existing solutions.

C. Security and Functionality Features

Table V presents the security and functionality features of the proposed protocol, and the same is compared with the existing protocols.

For this, we have considered various security features such as SF_1 : "resistance to replay attack", SF_2 : "resistance to man-in-the-middle attack", SF_3 : "resistance to privileged-insider attack", SF_4 : "resistance to impersonation attack", SF_5 : "resistance to physical vehicle capture attack", SF_6 : "resistance to session key disclosure attack", SF_7 : "resistance to known key secrecy attack", SF_8 : "resistance to sybil attack", SF_9 : "supports perfect forward secrecy", SF_{10} : "resistance to ephemeral secret leakage attack", and functionality features such as FF_1 : "support of mutual authentication", FF_2 : "support of RSU fault tolerance", FF_3 : "support of handover integrity", FF_4 : "preservation of anonymity", FF_5 : "preservation of untraceability", FF_6 : "support of decentralization (blockchain)", FF_7 : "support of security simulation", FF_8 : "support of multi-vehicular domain authentication", FF_9 : "support of handover authentication", FF_{10} : "suitable for large vehicular network". As examined in Section V, the proposed protocol ensures all

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

TABLE V
COMPARATIVE STUDY ON SECURITY AND FUNCTIONALITY FEATURES

Features	[12]	[13]	[17]	[18]	[19]	[27]	[28]	[29]	[30]	[31]	Ours
SF_1	O	O	O	O	O	O	O	O	O	O	O
SF_2	O	O	O	O	O	–	–	–	O	O	O
SF_3	–	–	O	–	O	–	–	–	–	O	O
SF_4	O	O	O	O	O	O	O	O	O	O	O
SF_5	–	–	–	–	–	–	–	–	–	O	O
SF_6	O	O	O	O	–	O	O	O	O	O	O
SF_7	O	–	O	O	–	–	–	–	O	O	O
SF_8	–	–	–	–	–	–	–	–	–	–	O
SF_9	–	–	O	O	–	–	O	O	O	O	O
SF_{10}	–	–	O	O	–	–	–	–	–	O	O
FF_1	–	–	O	X	X	O	X	O	X	O	O
FF_2	X	X	O	X	X	X	X	X	X	X	O
FF_3	X	X	O	O	O	X	X	X	X	X	O
FF_4	O	O	O	O	X	O	O	X	X	O	O
FF_5	O	–	O	X	X	O	O	–	X	O	O
FF_6	O	O	O	O	O	–	–	–	–	X	O
FF_7	–	–	O	O	X	–	O	–	–	O	O
FF_8	–	No	–	No	No	No	No	No	No	No	Yes
FF_9	O	O	O	O	O	O	O	O	O	–	O
FF_{10}	No	No	No	No	No	No	No	No	No	No	Yes

– : the scheme does not consider the feature (or) security solution against attack is not presented in the state-of-the-art; O: the protocol supports the feature (or) secure against applicable attack; X : the protocol does not support the functionality feature.

the presented security features. However, the scheme presented in [12], [13], [17], [18], [19], [27], [28], [29], and [30] do not consider all security and functionality features. From Table V, it is clear that the proposed protocol can provide better security and functionality features than the existing protocols. The proposed protocol supports multi-vehicular domain authentication of vehicles, and it can also be suitable for large vehicular networks.

VII. CONCLUDING REMARKS & FUTURE SCOPE

In this article, we have designed a blockchain-based V2R mutual authentication and session-key agreement protocol based on the ECC and hash function. The proposed protocol establishes secure communication when the vehicles and RSU communicate in the intra-vehicular and inter-vehicular regions. This solution provides substantially less computation concerning the vehicle whenever the handover scenario arises in the inter-vehicular case. As a result, our proposed scheme can increase the efficiency of the transportation system. Moreover, we have considered two blockchain and multi-domain scenarios while developing the protocol. Therefore, it can be suitable for a large vehicular network. The protocol is informally investigated, which proves that it is secure. Furthermore, to show the robustness of the proposed solution against attacks, the ROR model and Scyther tool as formal security analysis and verification have been used. Finally, the detailed comparative analysis of the proposed protocol with state-of-the-art confirms that our scheme has superior functionality and security features and requires justifiable communication and computation costs. In future work, we plan to implement the proposed system using the NS-3 (or) Veins simulator and enhance the system's efficiency and security. Additionally, our research team will try to execute blockchain implementation in external test networks.

REFERENCES

[1] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 12, pp. 1913–1922, Dec. 2021.

[2] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, May 2020.

[3] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, Feb. 2021.

[4] B. D. S. Sai, R. Nikhil, S. Prasad, and N. Srinivas Naik, "A decentralised KYC based approach for microfinance using blockchain technology," *Cyber Secur. Appl.*, vol. 1, 2023, Art. no. 100009.

[5] S. K. Dwivedi, R. Amin, S. Vollala, and R. Chaudhry, "Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities," *Comput. Elect. Eng.*, vol. 86, 2020, Art. no. 106719.

[6] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.

[7] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.

[8] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15824–15838, Jul. 2021.

[9] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. Park, "Block-CLAP: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8092–8107, Aug. 2021.

[10] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular *ad hoc* networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[11] Y. Zhao, Y. Wang, P. Wang, and H. Yu, "PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV," *IEEE Syst. J.*, vol. 16, no. 2, pp. 3422–3432, Jun. 2022.

[12] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Third Quarter 2021.

[13] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, 2021.

[14] P. K. Sharma and J. H. Park, "Blockchain-based secure mist computing network architecture for intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5168–5177, Aug. 2021.

[15] G. Li, W. Chen, B. Zhang, and S. Lu, "A fine-grained anonymous handover authentication protocol based on consortium blockchain for wireless networks," *J. Parallel Distrib. Comput.*, vol. 157, pp. 157–167, 2021.

[16] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, "Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment," *J. Syst. Architecture*, vol. 115, 2021, Art. no. 102024.

[17] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May/Jun. 2022.

[18] F. Yu, M. Ma, and X. Li, "A blockchain-assisted seamless handover authentication for v2i communication in 5G wireless networks," in *Proc. IEEE Int. Conf. Commun.*, 2021, pp. 1–6.

[19] Q. Li, W. Su, P. Zhang, X. Cheng, M. Li, and Y. Liu, "Blockchain-based method for pre-authentication and handover authentication of IoV vehicles," *Electronics*, vol. 12, no. 1, 2022, Art. no. 139.

[20] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.

[21] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2001, pp. 453–474.

[22] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 388–397.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.

[23] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[24] P. Mall and R. Amin, "EuDaimon: PUF-based robust and lightweight authenticated session key establishment protocol for IoT-enabled smart society," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2891–2898, Jun. 2022.
[25] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.*, 2005, pp. 65–84.
[26] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar./Apr. 2020.
[27] T. Gao, X. Deng, N. Guo, and X. Wang, "An anonymous authentication scheme based on PMIPv6 for VANETs," *IEEE Access*, vol. 6, pp. 14686–14698, 2018.
[28] C. Xu, X. Huang, M. Ma, and H. Bao, "An anonymous handover authentication scheme based on LTE-A for vehicular networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, 2018.
[29] Y. Jiang, S. Ge, and X. Shen, "AAAS: An anonymous authentication scheme based on group signature in VANETs," *IEEE Access*, vol. 8, pp. 98986–98998, 2020.
[30] T. Gao, X. Deng, Q. Li, M. Collotta, and I. You, "APPAS: A privacy-preserving authentication scheme based on pseudonym ring in VSNs," *IEEE Access*, vol. 7, pp. 69936–69946, 2019.
[31] P. Bagga, A. K. Das, and J. J. P. C. Rodrigues, "Bilinear pairing-based access control and key agreement scheme for smart transportation," *Cyber Secur. Appl.*, vol. 1, 2023, Art. no. 100001.

Sanjeev Kumar Dwivedi (Student Member, IEEE) is currently working toward the Ph.D. degree with the Department of CSE, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. He has a total academic experience of 4 years. He has authored or coauthored few research papers in Journals and Conference proceedings of International reputes. His research interests include information security, cryptography, blockchain technology.

Ruhul Amin (Senior Member, IEEE) is currently an Assistant Professor with the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. He has authored many technical research papers. Some of his research findings are published in top cited journals such as IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE INTERNET OF THINGS, and *Ad-HoC Networks*. He has been included in the subject-wise ranking of top 2 percent scientists from India (all fields) in the area of Networking and Telecommunications. His research interests include cryptography and network security, authentication protocol, and blockchain technology. He is also an Associate Editor for *Security and Privacy Journal* published by John Wiley.

Satyanarayana Vollala (Member, IEEE) is currently an Assistant Professor with the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. His research interests include security protocols, number system, hardware implementations public-key cryptography and modular exponential algorithms.

Muhammad Khurram Khan (Senior Member, IEEE) is currently a Professor of cybersecurity with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia. He is Founder and CEO of the Global Foundation for Cyber Studies and Research (http://www.gfcyber.org), an independent and nonpartisan cybersecurity think-tank in Washington D.C, USA. He is an Inventor of 10US/PCT patents. His research interests include cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is on the Editorial board of several journals which include IEEE COMMUNICATIONS SURVEYS & TUTORIALS, IEEE COMMUNICATIONS MAGAZINE, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, *Journal of Network & Computer Applications (Elsevier)*, IEEE ACCESS, IEEE CONSUMER ELECTRONICS MAGAZINE, *PLOS ONE*, and *Electronic Commerce Research*. He is a Fellow of the IET (U.K.), BCS (U.K.), and FTRA (Korea). He is a distinguished Lecturer of the IEEE.

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY ROORKEE. Downloaded on April 18,2024 at 12:21:24 UTC from IEEE Xplore. Restrictions apply.