IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 17 March 2023, accepted 30 March 2023, date of publication 10 April 2023, date of current version 14 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3265959

RESEARCH ARTICLE

BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment

SULAIMAN M. KARIM[1], ADIB HABBAL[1], (Senior Member, IEEE), SHEHZAD ASHRAF CHAUDHRY[2], AND AZEEM IRSHAD[3]

[1]Department of Computer Engineering, Faculty of Engineering, Karabük Üniversitesi, 78050 Karabük, Turkey
[2]Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates
[3]Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan

Corresponding author: Sulaiman M. Karim (suleymankerim@ogrenci.karabuk.edu.tr)

The work of Shehzad Ashraf Chaudhry was supported by the Abu Dhabi University's Office of Research and Sponsored Programs under Grant 19300810.

ABSTRACT The Internet of Vehicles (IoV) is a network that connects vehicles and their environment: in-built devices, pedestrians, and infrastructure through the Internet using heterogeneous access technologies. During communication between vehicles, roadside units, and control rooms, data confidentiality and privacy are critical issues that require effective measures. Several works have been proposed for securing IoV environments based on vehicles-to-infrastructure authentication; However, some schemes have security vulnerabilities, while others have shown efficiency issues. Due to its decentralization, stability, and transaction tracking capabilities, Blockchain as an emerging technology presents a potential solution for IoV security. This article provides an in-depth examination of the benefits of blockchain for a 5G-based IoV environment. In particular, we propose and evaluate a novel blockchain-based secure data exchange (BSDCE-IoV) scheme based on Elliptic Curve Cryptography algorithm. Our solution is designed to eliminate several potential attacks that pose a threat to the IoV environment. Deep examination using the Real-or-Random oracle model and Scyther tool, in addition to the informal security analysis, validates the scheme regarding security and privacy. The Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) assesses the computational and communication overhead. Computational and communicative overheads were also evaluated using the Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). BSDCE-IoV shows higher performance in terms of security, functionality, and time delay than a number of recent selective work in IoV security.

INDEX TERMS IoV, blockchain, security, authentication, V2V communication.

I. INTRODUCTION

The vehicular network is evolving toward a new concept, the IoV. IoV is an entirely dynamic network that utilizes wireless channels to link vehicles, users, and network infrastructure to the Internet [1]. The IoV network operations involve several communication entities, including vehicles, roadside units (RSUs), control rooms (CR), registration authority (RA), and pedestrians. Heterogeneous access technologies are used for communications by the entities inside the IoV environment [2]. Connected vehicles are becoming an essential face of the next generation of Intelligent Transportation Systems (ITS). Vehicle-to-everything (V2X) communications are used in various applications to improve traffic and vehicle performances and exchange traveling experiences. These applications include traffic control, system efficiency enhancement, and transportation system environmental sustainability [3], [4].

The potential applications are expanded by integrating 5G technology with IoV networks. The widespread use of

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

5G's diverse applications has diversified the demands for quality of service (QoS) and intelligent deep learning applications, making IoV easier and more standardized. Most smart applications need excellent reliability, exceptionally high data throughput, scalability, and minimum delay, which 5G technology can provide [5]. By enabling vehicular network capabilities for extremely high performance, the 5G network provides the basis for developing an intelligent IoV environment [6]. Additionally, the IoV network is more dependable and scalable because of 5G's expanded communication range compared to the Dedicated Short-Range Communication (DSRC) protocol range. As vehicles are expected to contribute to the Social Internet of Vehicles (SIoV), Smart City and ITS, 5G technology provide a highly leading role [7], [8].

The Internet of Things (IoT) is the most promising technology in recently developed applications, including those in business, healthcare, agriculture, energy management, security, and other areas [9], [10]. IoT uses involve gathering, enabling, and sharing anonymous data from industrial equipment, vehicles, smart homes, and other smart devices. Over 8.4 billion new devices joined the IoV worldwide network in 2017, a 31% increase from 2016, demonstrating the active growth of the IoT's connected devices [11]. The IoV's vehicles are equipped with a wide variety of smart devices, including radar, cameras, GPS, and other sensors. A range of networks and protocols, including 5G, are employed to connect and share information. A vehicle can then collect the outgoing data, process it, and send it to another vehicle or the RSU using wireless communication technologies like Wi-Fi, DSRC, and 5G.

From the debut of the first generation (1G) in 1980 to the current operational 5G, mobile communication technology has evolved. Even though 1G was at the time considered a true breakthrough in communication, it had several flaws, including poor sound quality, coverage issues, device weight, battery life, and security. Digital switching, SMS, and voice encryption were all features of the second generation (2G) that was first deployed in 1990. However, this technology had several drawbacks, including limited hardware capabilities, poor mobility, and low data rates. The third generation (3G) system, which promoted novelties like interactive media messaging, position monitoring, Internet surfing, and improved security protocols, was introduced in 2001, marking a significant stride forward. Nonetheless, this generation still has many negative aspects due to the expensive equipment. The rollout of the fourth generation (4G) began in 2010, and it included better features such as a faster data rate, minimal delay, high-definition video (HDV), and voice-over IP (VoIP) [12]. The latest mobile system generation, 5G, has been available since 2020. It offers faster Internet speeds as well as several new capabilities for multimedia use, dependability, secure protocols, and extended range [13]. The building blocks for supporting the outdated 2G, 3G, 4G, and Wi-Fi platforms are provided by 5G mobile technology [14], [15]. Even though the fifth generation (5G) of mobile technology is currently in use, scientific study has started to explore the anticipated advancements in communications, particularly information security, in the sixth generation (6G) mobile system. Compared to its predecessors, 6G will provide a more extensive connection-aware network service, lower latency, and greater flexibility [16].

IoVs use mobile communication technologies to allow vehicles to forward information to different infrastructures, such as RSUs and CRs [17]. 5G-mobile contributes to IoV environment communication in activities between V-to-RSU, RSU-2-CR, and CR-2-RA. During V2V communication or, more generally, V2I, security/ privacy is a critical issue that presents a real threat to the system and requires practical solutions. Due to the movement of vehicles, many types of external and internal cyberattacks challenge the IoV environment. Figure 1 shows the influencing elements of the blockchain (BC) envisioned IoV system, namely the vehicles, RSUs, CRs, RA, and blockchain center.

A. THREAT MODEL

Because the IoV uses an unprotected wireless communication channel, an attacker can launch forgery attacks against vehicles or RSUs. For the newly proposed scheme's security validation, the well-known threat pattern known as the "Dolev-Yao (DY model) model" is employed [18]. In this pattern, an attacker can perform various forgery attacks by intercepting, altering, blocking, replaying, or deleting messages transmitted between communicating parties.

The De facto CK-adversary model has also been considered for further examination because an attacker has additional power with this pattern, allowing him to acquire session keys, random secrets, and long-term credentials [19]. It is confirmed that to protect against attacks on ephemeral information and forward secrecy attacks, the session key agreed upon by the cars and RSU entities must include both short-term random secrets and long-term credentials. Long-term and short-term secrets are both used to resist such attacks.

B. RESEARCH CONTRIBUTIONS

A new trustable and reliable authentication is introduced to improve information security in IoV based on Elliptic Curve Cryptography (ECC). Added to its approved security, it accomplishes mutual authentication with a minimum time cost. The main objective of this study is to propose a Blockchain-based Secure Data Collection and Exchange scheme for IoV (BSDCE-IoV) in 5G environment. In particular, we achieve the following contributions:

- The importance of secure data exchange between system components in a 5G-enabled IoV environment is discussed. The proposed communication model contributes to the understanding of the threats against IoV.
- Improved information security in IoV by a novel, trustable, and reliable authentication procedure between vehicles and RSUs is achieved.
- BSDCE-IoV is a new scheme that enables in establishing the authenticated key agreements (AKAs) between

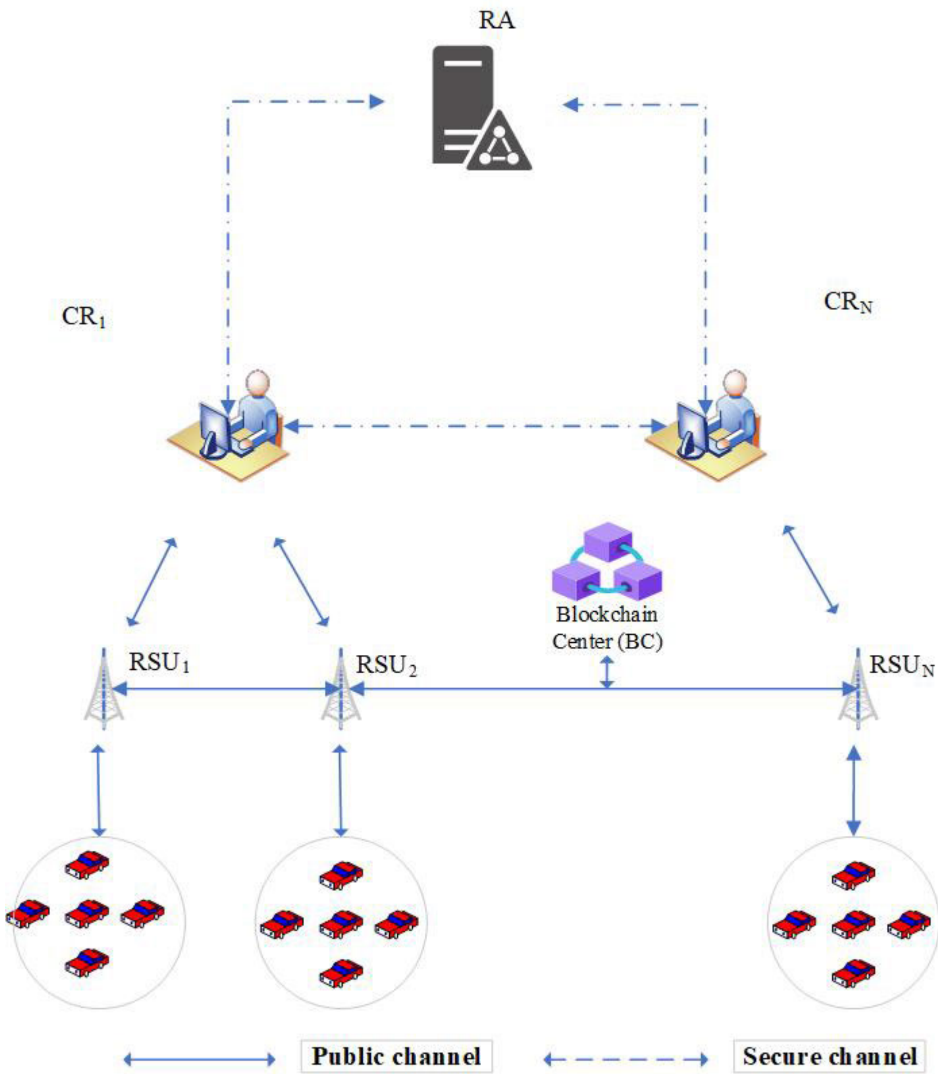


FIGURE 1. IoV componente registration.

vehicles and RSUs in each driving zone (DZ). Vehicles-RSU session keys can be set up to conduct secure communication based on a specified AKA technique. The scheme's data transmission and collection procedure enable the recording of all associated transactions involving vehicles, RSUs, and CRs to use RSUs to create private blocks.

- A Chosen leader from RSUs verifies and adds new blocks to the blockchain network using a consensus-based algorithm.
- For calculating the execution time, the well-approved collection of cryptographic primitives "Multi-precision Integer and Rational Arithmetic Cryptographic Library" (MIRACL) is used.

C. PAPER LAYOUT

A short survey about related works is presented in section II. Section III reviews the proposed BSDCE-IoV scheme with all its sub-phases. While section IV describes the use of blockchain. Informal/ formal security analysis is depicted in section V. In section VI, MIRACL empirical results are discussed. A comparative study is conducted in section VII. Finally, the paper is concluded.

II. RELATED WORK

As an active research area, IoV security has recently seen several proposed access control schemes. Authentication was among the most rated proposed solutions added to the blockchain as an emerging technology. To make sure that a connected vehicle can be believed to be who they claim to be, approved IoV authentication is necessary. Consequently, the implication of strong authentication is considered the most crucial step toward an IoV secure environment [20]. In such an attempt, [21] introduced an authentication scheme based on three-factor, where a physical unclonable function has been proposed for authentication and key exchange.

This function combined with password and biometrics to ensure robust authentication in IoV. The suggested protocol successfully counters de-synchronization attacks and many other challenges, as indicated by a convenient security analysis. A re-evaluation of this solution was carried out by [22], where vulnerabilities and limitations were identified concerning security. The attacker was able to find the mutual session keys of the vehicle user and vehicle data center, according to a systematic investigation used to identify the exposure. A secure update is proposed to overcome this severe threat.

A new authentication protocol is envisioned based on the ECC algorithm with a new distributed digital signature to secure IoV [23]. RSUs and vehicles generate the signature to reduce the workload of Trusted Authority (TA). Theoretical analysis proves the efficiency of the protocol as TA reveals its ability to track illegal messages and enforce system privacy. Using an ECC algorithm, the technique contributed in building a lightweight authentication protocol.

A new system, AKAP-IoV, supporting secure communication, mutual authentication, and key management among vehicles, RSUs, fog, and cloud servers, has been introduced [24]. Scyther and Tamarin have evaluated the proposed scheme performance, and a formal security analysis using the Real-or-Random (RoR) oracle model proved effective against threats.

A blockchain-based authentication and key agreement protocol are proposed for the multi-Trusted Authority (TA) network model [25]. The TA computing load is transferred to the RSUs, increasing authentication efficiency. Additionally, blockchain technology is used to manage the multiple TAs to manage the ledger storing vehicle information, making it possible for the vehicles to quickly accomplish cross-TA authentication with approved resistance against threats. An authentication scheme for IoV over blockchain based on ECC, hash function, and blockchain technique is introduced by [26]. A sequence of six consecutive steps, namely, initialization, registration, mutual authentication, key sharing, consensus, and certificate update, are included in the proposed scheme. It may accomplish confidentiality, integrity, authenticity, privacy, anonymity, non-repudiation, and perfect secrecy. Therefore, it is resistant to assaults like DDoS, replay, man-in-the-middle, identity theft, traffic analysis, masquerading, and session key disclosure attacks.

A secure consensus algorithm called SG-PBFT, based on the distributed blockchain is proposed to solve the problem of the limited computing power of the IoV [27]. It considers efficiency and system security by groping nodes according to their scores. The experimental findings demonstrate that in terms of transaction delay, throughput, and communication overhead, SG-PBFT is superior to many other schemes. CyberTwin technology is combined with blockchain to propose a new efficient authentication, namely CyberChain, to answer the limitation problem of communication and storage in IoV [28]. It accomplishes system privacy, communication efficiency, and minimum authentication delay through a new consensus mechanism. The simulation highlights the merit of the proposed CyberChain by ensuring almost identical security while reducing caching costs by 50% when compared to classical blockchain. In [29], a safe and effective blockchain-envisioned authentication protocol for IoV called SEA is presented. The scheme achieves mutual authentication among vehicles, edge nodes, and cloud servers. Additionally, edge nodes carry out vehicle authentication by checking the blockchain for the recorded authentication result, which minimizes cryptographic computation and communication overhead.

An approved key management scheme called AKM-IoV is proposed to ensure secure communication between vehicles, RSUs, Fog, and cloud servers in an IoV environment [30]. The authors stated that by using a formal (RoR) oracle model, an informal security analysis model, and the AVISPAs tool, the AKM-IoV confirmed its efficiency, functionality, and safety compared to other current protocols. However, weaknesses against vehicles, fog servers, RSU, and Cloud server impersonation attacks have been found [31]. Based on the Zero-knowledge proof (ZKP) and ECC, an innovative anonymous authentication method for IoV has been suggested [32]. The Trusted Authority can track the user's keys, ensuring the violation identification. The proposed method offers security, anonymity, mutual authenticity, unlikability, traceability, and resistance to replay assaults, albeit at a minor cost overhead increase. Using lattice cryptography, [33] has proposed a certificateless authentication protocol, enabling security for IoV resistant against quantum attacks. Further, a reliable blockchain model is presented, guaranteeing vehicles' trustworthiness in batch data verification.

The authentication system (A-MAC) has been presented based on a novel five-layer communication architecture to solve security challenges in the IoV environment [34]. The hash function is employed to maintain a high level of security while protecting the privacy and integrity of the data. A multi-level blockchain-based privacy-preserving authentication protocol is introduced in [23]. A global authentication center (GAC) for vehicle information archiving and a Local Authentication Center (LAC) for maintaining the blockchain are proposed in the architecture. There is also cluster formation, membership, cluster-head selection, and merging and leaving methods.

In [35], lightweight authentication is presented for emergency vehicles using a trusted authority as a central point. The proposed protocol is based on the strategy that a vehicle is mutually authenticated in its first integration to the IoV environment with the closest RSU using an authentication protocol. After that, re-authentication of the vehicle with the next RSUs is accomplished with less computing operation, which contributes to a decrease in the time cost. We believe that not repeating the entire authentication process for every RSU and using a central point of trustee (TA) presents a weakness in this scheme.

TA is used as a central decision point for the proposed authentication for the VANETs system [36]. This scheme attempts to solve the efficiency and latency issues of using identity-based authentication protocols. It presents an Identity-Based conditional authentication scheme to preserve privacy that does not depend on ideal Tamper-Proof Devices. The proposed scheme has proved to be safe against key leakage attacks and efficient in terms of time costs.

The use of TA usually complicates the mutual authentication process and introduces time overhead. In [37], mutual authentication is proposed for group communication on VANET without trusted authority. Furthermore, the proposed approach encrypts all messages before transmission and uses pseudonyms for identity secrecy. The suggested system is resilient against several security assaults, according to formal and informal security assessments.

Reference [38] focuses on mutual authentication with anonymity and intractability since it is essential to maintaining user privacy and information security in mobile edge computing. It is an identity-based authentication adapted to mobile computing, which has a great similarity to the IoV environment. This scheme accomplishes mutual authentication in a very short operation, "only a single message exchange round."

A scheme based on blockchain technology for mutual authentication and key-sharing for edge-computing-based smart grid systems is proposed in [39]. The scheme offers practical conditional anonymity and key sharing by utilizing blockchain. The protocol provides a respectable level of security according to the security analysis. We selected this work as part of the comparison with our paper, conducted in the next section because it is an important study in the field of IIoT area. It this important to compare and correlate our results not only with IoV security but with other IoT varieties.

Due to the base station's high density in the 5G network, repeated vehicle-to-RSU mutual authentication is necessary, which is reflected negatively on the network efficiency. A new blockchain-based scheme is proposed that accomplishes mutual authentication and key-sharing among vehicles and base stations with reduced time cost [40]. Scyther is used to validate the secrecy of the proposed protocol.

A similar approach to eliminate computing overhead by considering the handover situation is presented in [41]. To decrease the need for over-calculations during re-authentications and to enable vehicle revocation, a blockchain-based VANET protocol has been introduced. Due to the decentralized nature of blockchain, there is no need for a Trusted Authority in this scheme. The practicableness and security of the protocol have been validated using NS-3, AVISPA, (RoR) oracle model, and BAN logic. This scheme focused on reducing time costs and did not give importance to the security and privacy of information by designing a lightweight authentication.

Related works can be summarized as authentication as a key point of IoV protection. Due to the real-time nature of the IoV network, the main goal becomes to design a secure and lightweight authentication system. Some works use multi-factor authentication like passwords and biometrics while others use algorithms like ECC, and hash functions. Two authentication strategies are adopted, central point using TA or distributed without TA. Blockchain as an emerging technology is being integrated into the security process, promoting the use of distributed authentication in many recent works. Performance evaluation of proposed schemes includes formal and informal security analysis and tools such as AVISPA.

TABLE 1. Symbol and abbreviations.

SYMBOL	ABBREVIATIONS
V_n	n^{th} Vehicle
RSU_j	j^{th} Roadside Unit
CR_i	i^{th} Control Room
RA	Registration Authority
DC	Blockchain
h(.)	One Way Hash Function
E_p (a,b)	ECC polynomial
G	Generator or base point in E_P (a,b)
$Pr\text{-}K_{RA}$	Private key for RA
Pub_{RA}	public key for RA
ID_{RA}	RA Identity
ID_{CR}	CR Identity
$Pr\text{-}K_{CR}$	Private key for every CR_i
Pub_{CR}	Public key for every CR_i
$Certif_{CR}$	Unique certificate for every CR_i
MK_{CR}	Master key for every CR_i
PK_{CR}	Public key for every CR_i
ID_{RSU}	RSU identity
RID_{RSU}	Pseudo-identity of RSU_j
$Pr\text{-}K_{RSU}$	private key of RSU_j
Pub_{RSU}	Public key of RSU_j
$Certif_{RSU}$	Certificate for every RSU_j
MK_{RSU}	Second private key of RSU
PK_{RSU}	Public key of RSU - with MK
ID_V	Unique identity for every V_n
RID_V	pseudo-identity of V_n
$Pr\text{-}K_V$	private key of V_n
Pub_V	public key of V_n
SK_V	private key for signature of V_n
Pk_V	public key for signature of V_n
$Certif_V$	certificate for every V_n
Skey	session key
Skey-Ver	session key verification
Dsign	Digital signature
R_1,R_2	Random numbers
DHKey	Diffie-Hellman Key
ACK	Acknowledgement

III. BSDCE-IoV: BLOCKCHAIN-BASED SECURE DATA COLLECTION AND EXCHANGE SCHEMES

BSDCE-IoV is a multi-phase scheme where all system components, such as timestamps, are assumed to be synchronized. Table 1 explains the symbols and abbreviations used in this research.

A. PARAMETERS INITIALIZATION

This phase is performed by the RA. It starts by selecting necessary parameters for a non-singular ECC such as

TABLE 2. Registration operations summary.

Registration of CRs	
RA	CR
- RA is selecting E_p (a,b) , h (.) , G - RA selects a unique identity ID_{RA}, and a random private key Pv_{RA}, then calculate $Pub_{RA} = Pv_{RA}.G$. - RA selects a unique identity ID_{CR_i} for every CR and random private key for CR_{CR_i} = $Pr\text{-}K_{CR_i} \in Z_p^*$, and computes $Pub_{CR_i} = Pr\text{-}K_{CR_i}$ .G . - RA create a unique certificate for CR_{CR_i} : $Certif_{CR_i} = Pr\text{-}K_{CR_i} + h(ID_{CR_i} \parallel ID_{CR_i} \parallel Pub_{RA} \parallel Pub_{CR_i}) * Pv_{RA}$ (mod p) - RA deletes $Pr\text{-}K_{CR_i}$	- CR_i selects a master key $MK_{CR_i} \in Z_p^*$, and computes the public key $PK_{CR_i} = MK_{CR_i}$ .G. - { ID_{CR_i} ,ID_{RA},$Certif_{CR_i}$,MK_{CR_i} ,PK_{CR_i} ,Pub_{RA},Pub_{CR_i},E_p (a,b) , h (.) , G }is stored.
The information {PK_{CR_i}, Pub_{RA} , Pub_{CR_i} ,E_p (a,b) , h (.) , G } is published as public	
Registration of Roadside Units (RSUs)	
CR	RSU
- CR_i selects a unique identity for every $RSU_j = ID_{RSU_j}$, and computes the pseudo-identity $RID_{RSU_j} = h(ID_{RSU_j} \parallel MK_{CR_i})$ - CR_i selects the private key $Pr\text{-}K_{RSU_j} \in Z_p^*$. CR_i calculates $Pub_{RSU_j} = Pr\text{-}K_{RSU_j}$ .G - The certificate: $Certif_{RSU_j} = Pr\text{-}K_{RSU_j} + h(RID_{RSU_j} \parallel Pub_{RSU_j} \parallel Pub_{CR_i}) * MK_{CR_i}$ (mod p) is created - CR_i stores RID_{RSU_j} and $Certif_{RSU_j}$ stores RID_{RSU_j} and $Certif_{RSU_j}$ - CR_i deletes the ID_{RSU_j} and $Pr\text{-}K_{RSU_j}$ for security reason	- RSU_{RSU_j} selects $MK_{RSU_j} \in Z_p^*$, and computes $PK_{RSU_j} = MK_{RSU_j}$ .G - CR_i preload to RSU_{RSU_j} { RID_{RSU_j} , ID_{CR_i} , $Certif_{RSU_j}$, ID_{RSU_j} , Pub_{CR_i} ,Pub_{RSU_j} , (MK_{RSU_j} , PK_{RSU_j}),PK_{CR_i},E_p (a,b) , h (.) , G }
The information {PK_{RSU_j}), Pub_{RSU_j} }is published as public	
Vehicles Registration	
CR	Vehicle (V)
- ID_{V_n} is selected, $RID_{V_n} = h(ID_{V_n} \parallel MK_{CR_i})$ - CR_i selects randomly $Pr\text{-}K_{V_n} \in Z_p^*$, and compute $Pub_{V_n} = Pr\text{-}K_{V_n}$.G - A certificate for every V_n is created: $Certif_{V_n} = Pr\text{-}K_{V_n} + h(RID_{V_n} \parallel Pub_{V_n} \parallel Pub_{CR_i}) * MK_{CR_i}$ mod(p) - ID_{V_n} and $Pr\text{-}K_{V_n}$ are deleted for security reason	- V_n selects, a private signature key: $SK_{V_n} \in Z_p^*$, computes $Pk_{V_n} = SK_{V_n}$.G - The stored credentials are: { RID_{V_n} ,$Certif_{V_n}$,Pub_{V_n}) ,(SK_{V_n} , Pk_{V_n}),Pk_{CR_i} ,E_p (a,b) , h (.) , G }.
The information {Pub_{V_n}, Pk_{V_n} }is published as public	

p (prime number) and an ECC function E_p (a, b): $y^2 = x^3 + ax + b$, where the constants a, and b $\in \{1, 2, \ldots, p-1\}$ with the non-singularity condition: $(4a^3 + 27b^2 \neq 0)$ A private key (Pv_{RA}), and an Identity (ID_{RA}) are also selected. A generator or base point (G) is chosen to generate the public key $Pub_{RA} = Pv_{RA}.G$. SHA-256 is used as a hash function for the scheme. The RA keeps its secret Pv_{RA} and publishes the other parameters E_p (a, b), G, Pub_{RA}, h(.).

B. IoV COMPONENTS REGISTRATION

The registration phase is composed of several sub-phases, as shown in the figure. 2, that is executed offline, assuming secure channels. The registration of CRs is performed by RA, while the registrations of RSUs and vehicles (Vs) are executed by their corresponding CR. The step-by-step registration procedure is outlined in Table 2.

- Registration of CRs by RA: It is performed in steps by the RA as follows:
  Step-1: The RA selects a unique identity ID_{CR_i}, and a random private key $Pr\text{-}K_{CR_i} \in Z_p^*$ for every CR_i. The public key for CR_i is equal to $Pub_{CR_i} = Pr\text{-}K_{CR_i}.G$, where k.G is known as the elliptic-curve scalar multiplication. For k $\in Z_p^*$, the elliptic curve scalar multiplication is $k \cdot G = G + G + \cdots + G$ (k-times). RA creates a unique certificate for every CR_i as $Certif_{CR_i} = Pr\text{-}K_{CR_i} + h\ (ID_{CR_i} \parallel ID_{RA} \parallel Pub_{RA} \parallel Pub_{CR_i}) * Pv_{RA}$ (* is a multiplication-mod). RA then deletes the $Pr\text{-}K_{CR_i}$ form database for security matters.
  Step-2: RA preload to every CR_i the information: $\{ID_{CR_i}$, ID_{RA}, $Certif_{CR_i}$, Pub_{RA}, Pub_{CR_i}, E_p (a, b), h(.), G$\}$
  Step-3: CR_i chooses a master key $MK_{CR_i} \in Z_p^*$ and finds the associated public version of this key $PK_{CR_i} = MK_{CR_i}.G$. In the end RA publish PK_{CR_i}, Pub_{RA},Pub_{CR_i}, E_p (a, b), G, h(.) as open data. Record CR_i credentials as: ID_{CR_i}, ID_{RA}, $Certif_{CR_i}$, MK_{CR_i}, PK_{CR_i}, Pub_{RA}, Pub_{CR_i}, E_p (a, b), h (.), G
- Registration of RSU by CR_i:
  Step-1: CR_i selects a unique identity for every $RSU_j = ID_{RSU_j}$, CR_i Computes the pseudo-identity $RID_{RSU_j} = h(ID_{RSU_j} \parallel MK_{CR_i})$. CR_i selects a random private key: $Pr\text{-}K_{RSU_j} \in Z_p^*$ and compute its corresponding public key

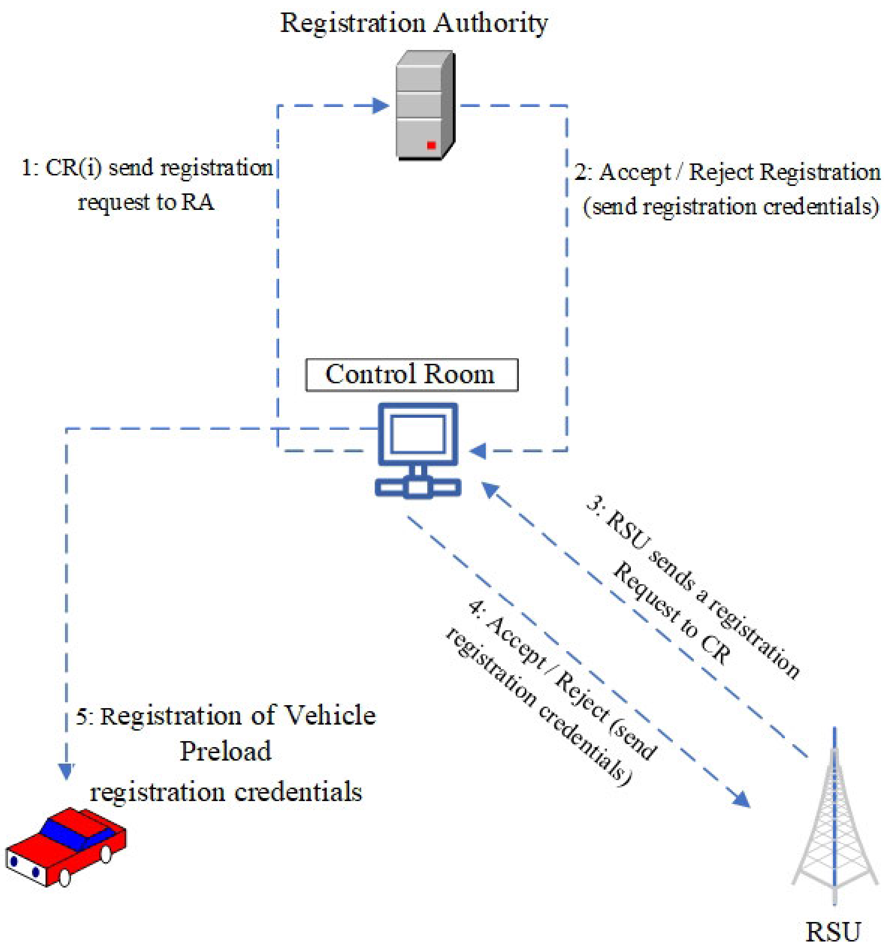


FIGURE 2. IoV componente registration.

$Pub_{RSU_j} = Pr\text{-}K_{RSU_j}.G$. A certificate for every RSU_j is created as $Certif_{RSU_j} = Pr\text{-}K_{RSU_j} + h\,(RID_{RSU_j} \,\|\, Pub_{RSU_j} \,\|\, Pub_{CR_i} * MK_{CR_i}$ (mod p).

Step-2: CR_i stores RID_{RSU_j} and $Certif_{RSU_j}$ in its database, and publishes Pub_{RSU_j} as public, then deleting ID_{RSU_j} and $Pr\text{-}K_{RSU_j}$ to guarantee data security.

Step-3: RSU_j selects a master key (private key) for decryption: $MK_{RSU_j} \in Z_p^*$. RSU_j, and computes the public key $PK_{RSU_j} = MK_{RSU_j}.G$.

Step-4: CR_i preload to the corresponding RSU_j credential info: RID_{RSU_j}, ID_{CR_i}, $Certif_{RSU_j}$, ID_{RSU_j}, Pub_{CR_i}, Pub_{RSU_j}, (MK_{RSU_j}, PK_{RSU_j}, PK_{CR_i}),E_p (a, b), h (.), G. CR_i makes public the information: PK_{RSU_j}, Pub_{RSU_j} . CR_i deletes the ID_{RSU_j} and $Pr\text{-}K_{RSU_j}$ for security reason.

- Registration of Vehicle V_n by CR_i:
  Before deployment of Vehicles in the DZ, every vehicle V_n must be registered by the corresponding CR as:
  Step-1: CR_i selects a unique identity for every $V_n = ID_{V_n}$ and computes the pseudo-identity of $RID_{V_n} = h\,(ID_{V_n} \,\|\, MK_{CR_i})$
  Step-2: CR_i selects a random private key for V_n certificate, $Pr\text{-}K_{V_n} \in Z_p^*$ and compute the public key $Pub_{V_n} = Pr\text{-}K_{V_n}.G$.
  Step-3: V_n selects a private signature key: $SK_{V_n} \in Z_p^*$, and calculates the corresponding public signature key $Pk_{V_n} = SK_{V_n}.G$.
  Step-4: CR_i creates a certificate for every V_n equal to $Certif_{V_n} = Pr\text{-}K_{V_n} + h\,(RID_{V_n} \,\|\, Pub_{V_n} \,\|\, Pub_{CR_i}) * MK_{CR_i}$ (mod p). After that, for security reason, CR_i deletes the ID_{V_n} and $Pr\text{-}K_{V_n}$. The credentials: RID_{V_n}, $Certif_{V_n}$, Pub_{V_n}, (SK_{V_n}, Pk_{V_n}, Pk_{CR_i}, E_p (a, b), h (.), G is stored in V_n. Finally, Pub_{V_n}, Pk_{V_n} are both published as public information.

C. AUTHENTICATION STRUCTURE

The mutual authentication is performed in two levels which are V-2-RSU and RSU-2-CR, by the proposed scheme. BSDCE-IoV is based on ECC. It includes mutual authentication and the establishment of a secure session key for secure communication. The session key ($SKey_{V-RSU}$ is generated

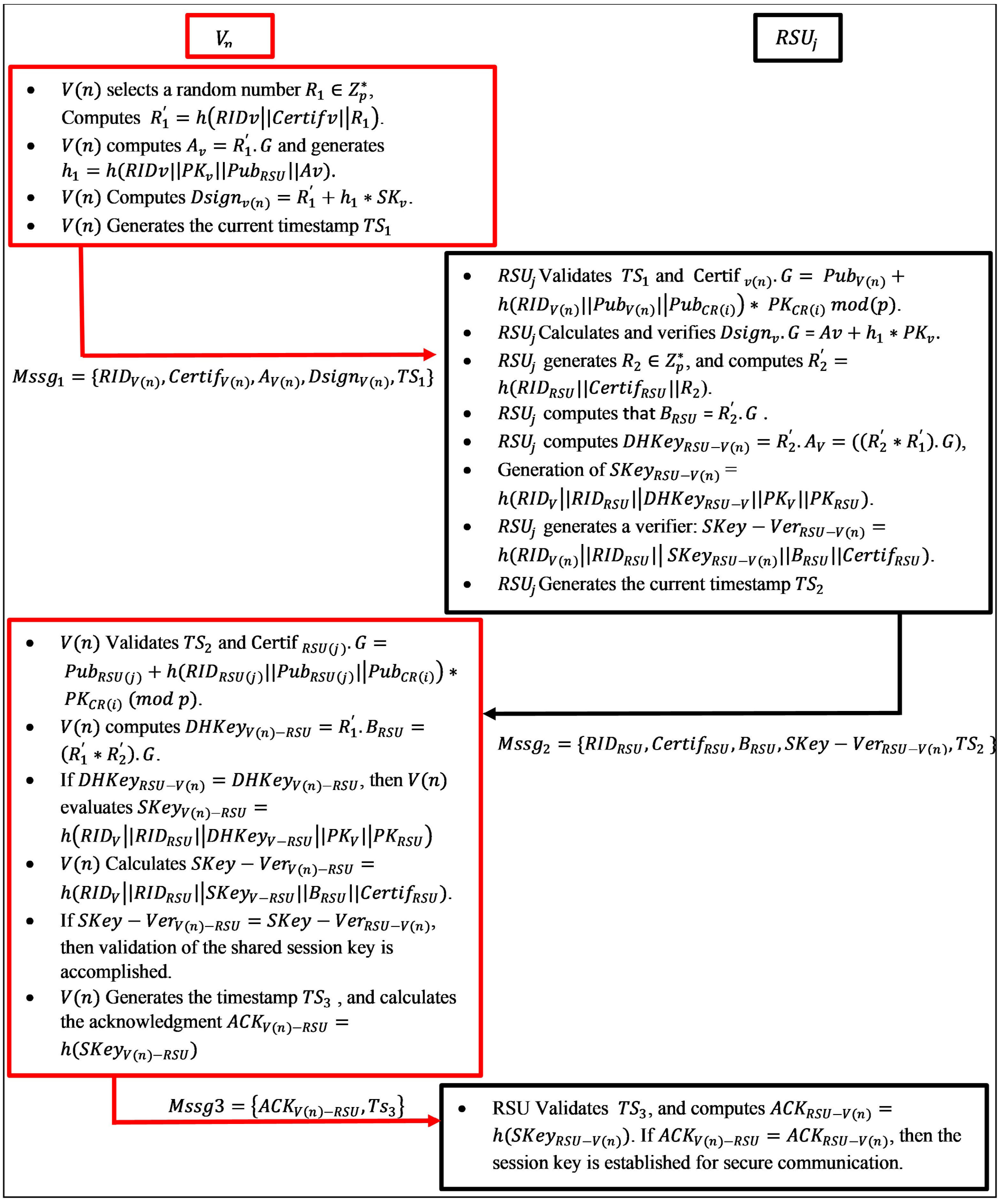


FIGURE 3. Mutual authentication.

using the ECC-Diffie- Hellman key exchange algorithm. Also, a session key verification digital signature is used (Skey-Ver$_{V-RSU}$) for validation of SKey$_{V-RSU}$. The authentication steps are presented in the figure. 3.

Step 1 (Vn Parameters Generation): V_n selects a random number $R_1 \in Z_p^*$, and computes $R_1' = h\ (RID_{V_n} \parallel Certif_{V_n} \parallel R_1)$. V_n calculates the public version of R_1'; $A_{V_n} = R_1'.G$, and $h_1 = h\ (RID_{V_n} \parallel PK_{V_n} \parallel Pub_{RSU} \parallel A_{V_n})$. The next move, V_n makes computes a digital signature $Dsign_{V_n} = R_1' + h_1 * SK_{V_n}$. Finally, V_n sends a message to the RSU: $Mssg_1 = RID_{V_n}, Certif_{V_n}, A_{V_n}, Dsign_{V_n}, TS_1$ in public channel.

Step 2 (V_n Parameters Verification by the RSU): After receiving $Mssg_1$ the RSU checks the validity of the certificate by: $Certif_{V_n}.G = Pub_{V_n} + h\ (RID_{V_n} \parallel Pub_{V_n} \parallel Pub_{CR_i}) * PK_{CR_i}$ mod(p). This information (Pub_{V_n}, RID_{V_n}, Pub_{CR_i}, PK_{CR_i}) is public, so, RSU can compute $Certif_{V_n}.G$ from the available data, and that received in $Mssg_1$. If the two results are the same, V_n certificate validation is then accomplished. RSU goes to valid the $Dsign_{V_n}$ by calculating $Dsign_{V_n}.G = A_{V_n} + h_1 * PK_{V_n}$. Because A_{V_n}, and RID_{V_n} are received by $Mssg_1$, while other data are publicly available, the validity of $Dsign_{V_n}$ can be verified.

Step 3 (RSU Parameters Generation): RSU generates a random number $R_2 \in Z_p^*$, and computes $R_2' = h\ (RID_{RSU} \parallel Certif_{RSU} \parallel R_2)$. The corresponding public number of R_2' is calculated such that $B_{RSU} = R_2'.G$. RSU computes the Diffie-Hellman Key exchange as $DHKey_{RSU-V_n} = R'_2$. A_{V_n}=((R'_2*R'_1).G), and the session key is generated as $SKey_{RSU-V_n}$ = h(RID_{V_n} || RID_{RSU} || $DHKey_{RSU-V}$ || PK_{V_n} || PK_{RSU}. The RSU generates a verifier of session key as SKey-Ver_{RSU-V_n} = h(RID_{V_n} || RID_{RSU} || $SKey_{RSU-V_n}$ || B_{RSU} || $Certif_{RSU}$. Finally, RSU sends to V_n the message $Mssg_2$ = { RID_{RSU}, $Certif_{RSU}$, B_{RSU} ,SKey-Ver_{RSU-V}, TS_2}.

Step 4 (RSU Parameters Verification by V_n): V_n receives $Mssg_2$ and checks the validity of RSU certificate by calculating $Certif_{RSU_j}$.G = Pub_{RSU_j} + h(RID_{RSU_j} || Pub_{RSU_j} || Pub_{CR_i}) * PK_{CR_i}) (mod p). The elements (Pub_{RSU_j}, RID_{RSU_j}, Pub_{CR_i}, Pub_{V_n}, and PK_{CR_i}) are known, so, V_n can validate the RSU certificate by comparing the result from available data and that received in $Mssg_2$. V_n computes the Diffie-Hellman Key exchange using received and known data as $DHKey_{V-RSU}$ = R'_1. B_{RSU} = (R'_1*R'_2).G. It is clear that for correct and authenticate received data we have $DHKey_{RSU-V}$ = $DHKey_{V-RSU}$. V_n is using the calculated $DHKey_{V-RSU}$ to generate the session key $SKey_{V_n-RSU}$ = h(RID_{V_n} || RID_{RSU} ||$DHKey_{V-RSU}$ || PK_{V_n} || PK_{RSU}), that must be equal to $SKey_{RSU-V_n}$. To verify that, a local verifier SKey-Ver_{V_n-RSU} is calculated from available data as SKey-Ver_{V_n-RSU} = h(RID_{V_n} || RID_{RSU} || $SKey_{V-RSU}$ || B_{RSU} || $Certif_{RSU}$. SKey-Ver_{V_n-RSU} is compared with the received SKey-Ver_{RSU-V_n} in $Mssg_2$. If they are the same then the validity of the session key, and the verifier for both sides are accomplished.

Step 5 (Acknowledgment): V_n calculates the acknowledgment variable as

ACK_{V_n-RSU} = h($SKey_{V-RSU}$), and sends it in open channel $Mssg_3$ = ACK_{V_n-RSU}, TS_3 to RSU.

Step 6 (Acknowledgment Validation by the RSU): RSU computes ACK_{RSU-V_n} = h($SKey_{RSU-V_n}$). If ACK_{V_n-RSU} = ACK_{RSU-V_n}, then the session key is established correctly for future secure communication.

D. SECURE INFORMATION EXCHANGE

This section covers numerous data transmission and collection-related transactions between vehicles, RSUs, and the control room in the DZ. RSU is always part of these transactions:

- The data delivery request from CR_j to RSU_j is accomplished through the transaction $R_{CR_i-RSU_j}$. This request is encrypted by the public key PK_{RSU_j} of the target element, which is then decrypted by RSU_j using its private MK_{RSU_j} key.
- The transaction $R_{CR_i-RSU_j}$ is requesting information transmission between RSU_j and CR_j. The public key PK_{CR_i} is used to encrypt the transaction, while the decryption is executed using the private key of the CR_i; MK_{RSU_j}. The requested data can be informed of other RSUs or vehicles operating outside the DZ_j.
- The data delivery request from RSU_j to V_n using the encrypted transaction $R_{RSU_j-V_n}$. The encryption/ decryption process is performed by the established session key $SKey_{RSU-V}$ between RSU and V.
- The encrypted transaction $R_{V_n-RSU_j}$ is a data request from V_n to RSU_j. The encryption/ decryption of the transaction is performed by the established session key $SKey_{RSU-V}$. The information provided by the RSU_j concerns many activities like the traffic state and road information updated in the RSU_j by all connected vehicles within certain time limits.

IV. BLOCKCHAIN

Blockchain is a decentralized, public, distributed ledger-based system that records transactions across computer systems. It was developed as an underlying network for the crypto-currency system "Bitcoin". It has recently been adopted by various applications such as finance, the Internet of Things, energy management, logistics, and healthcare [42]. Unlike traditional databases, blockchain has no central governing authority and operates on a fully distributed peer-to-peer architecture. As a result, blockchain-based applications enjoy high data availability, trustworthiness, scalable environment, security, and privacy. For example, Blockchain enhances transaction transparency by requiring that each node maintain a complete copy of the database. Before updating their databases, participating nodes must approve each new transaction to reach a consensus. The self-executing code known as a "smart contract" operates independently of any central authority and is triggered once its criteria are met [43].

Three types of blockchain exist public, private, and consortium blockchains. The public Blockchain is a completely decentralized ledger open to everyone for membership, as in Bitcoin and Ethereum. A private blockchain is a permission-based technology that a private institution adopts. Centralized authority is necessary to approve and control the participation in this network and manage the restrictions of the writing and reading of blockchain members. Finally, a consortium, considered a hybrid type of blockchain, relies on a set of authorized entities to manage it. This type can use hybrid access technology, allowing authorized contact with the outside world [1].

blockchain has acquired significant research attention in ITS, including IoV to improve the driving experience by safely transferring data through V2X and enhancing system security and privacy. The mobile nature of the network and the variety of elements involved in the IoV environment results in a large amount of data. Therefore, blockchain technology has become a viable solution for IoV data security and privacy.

A. BLOCKS CREATION, ADDITION, AND VERIFICATION

RSU_i will create a block called $B_{(k)}$ utilizing the transactions that are accessible to RSU_i as shown in table 3. Several encrypted transactions utilizing the RSU_i public key can be found in block $B_{(k)}$ created by RSU_i. RSU_i uses the "elliptic curve digital signature algorithm (ECDSA)" to create the signature on the block [44].

The immutability and transparency of the created blocks in the blockchain are achieved through digital signature,

TABLE 3. Structure of a block k.

Previous Block Hash	PBH
Creator of Block	CB_{ID} (Identity of one of the RSUs, say RSU_j in P2P RSU network)
Merkle Tree Root	MTR
Block Version	BV_{er}
Timestamp	TS
Public key of Signer RSU_j	PK_{RSU_j}
Block Payload	(Encrypted Transactions)
List of tn Encrypted Transactions #i TS_i	{EPK_{RSU_j} TS_i | i=1,2,..,tn}
Current Block Hash	CBHash
Signature on CBHash	SCBHash

Merkle tree, and block hash root. A selection algorithm selects a leader (LD) in a point-to-point RSU network containing N number of RSU blockchain members [45]. According to the algorithm (1), a new block $B_{(k)}$ is submitted to the leader LD for consensus-building before it is verified and added to the blockchain [46]. The known "Practical Byzantine Fault Tolerance (PBFT)" technique is used as the consensus for this algorithm [47]. Stages 6-9 in figure 4 outline the general process of adding a block to the blockchain center, including block generation, verification, and insertion.

Smart contracts are computer programs with associated codes and data (their functions and state) that are executed and verified automatically without human intervention [48]. In blockchain, a smart contract is a program activated when certain pre-set conditions are met. The IoV system verifies and validates the "correct execution of the transactions" to the point of "legal contracts." The agreements and contracts between communication parties in the blockchain network include traceability, immutability, and irreversibility as fundamental characteristics.

Blockchain technology is distinguished from other technologies by its security, efficacy, cost-effectiveness, and resilience. In the presented BSDCE-IoV, the smart contract is implemented in all RSUs. It is used for vehicles, CRs, and other RSUs transaction verification, block creation, and addition in an IoV environment. A smart contract strategy protects against modification attacks on the IoV system data.

As a result, the data integrity and secrecy are evident results of using blockchain [49]. Therefore, besides smart contracts, blockchain technology contributes in securing information exchange between IoV system elements.

Algorithm 1 Block Insertion and Verification Consensus in the Blockchain

- Input: block B(k) as defined in Table. 3. NF_{RSU} is the number of faulty RSUs in the point-to-point RSU network.
- Output: Commit and add block B(k) to the blockchain network after validating it successfully as in the following steps:-

1) Suppose LD, let's say RSU(LD), is chosen to be BC-leader and that it wishes to add B(k) on the blockchain.
2) For each follower ground station server node RSU_j, LD creates a current timestamp TS_{RSU_j} and conducts voting.
3) Voting request VtoReq is encrypted by LD as PK_{RSU_j} (VotReq, Ts_{RSU_j}), and sent to each follower node RSU_j as $E_{PK_{RSU_j}}$ (VotReq, Ts_{RSU_j}), ($j = 1, 2, \ldots, N_{RSU}, j \neq LD$), E(.) is the encryption function, while D(.) is the decryption function.
4) Suppose that each follower RSU_j in the P2P RSU network receives the message from LD at time $TS^*_{RSU_j}$.
5) For every follower-node RSU_j do
6) message decryption: ($VtoReq'$, TS_{RSU_j}) $D_{MK_{RSU_j}}$ [$E_{PK_{RSU_j}}$ ($VotReq$, TS_{RSU_j})].
7) Verify the received block B(k) "timestamp, Merkle tree root, present block hash, and signature".
8) In case of successful verification, VotReq " the voting reply" and (BVS) " block verification status" are sent as $E_{pk_{LD}}$ ($VotReq'$, VotRep, BVS) to LD.
9) End for
10) If VCnut is the vote-counter, set VCnut $\leftarrow 0$.
11) For each received response message {$E_{pk_{LD}}$ ($VotReq'$, VotRep, BVS)} the responded follower RSU_j do
12) Calculate ($VotReq'$, VotRep, BVS) $= DK_{LD}$ [$E_{pk_{LD}}$ ($VotReq'$, VotRep, BVS)]
13) If ($VotReq' = VotReq$), ((VotRep = valid) and (BVS = valid)) then
14) Set VCnut = VCnut+1
15) End if
16) End for
17) If (VCnut > $2.NF_{RSU} + 1$) then
18) Send the commit response to all follower nodes
19) B(k) Block addition to the BC.
20) End

V. SECURITY ANALYSIS

BSDCE-IoV security has been tested and validated using two formal security analyses, the Scyther tool and the Real-or-Random oracle model. In addition, the classic, informal security analysis is used by analyzing attacks and countermeasures generated by BSDCE-IoV. It has been proven that the algorithm is secure.

A. INFORMATION SECURITY ANALYSIS

- Replay Attack: - Provide a time synchronizer in the Transmission-reception and compare the time difference with a selected T_1 (timestamp). Also, it is impossible due to the use of secret random values (R_1, R_2).
- Man-in-the-Middle Attack: - Without the credential of V_i, an eavesdropper cannot generate $Dsign_{v_i}$ because

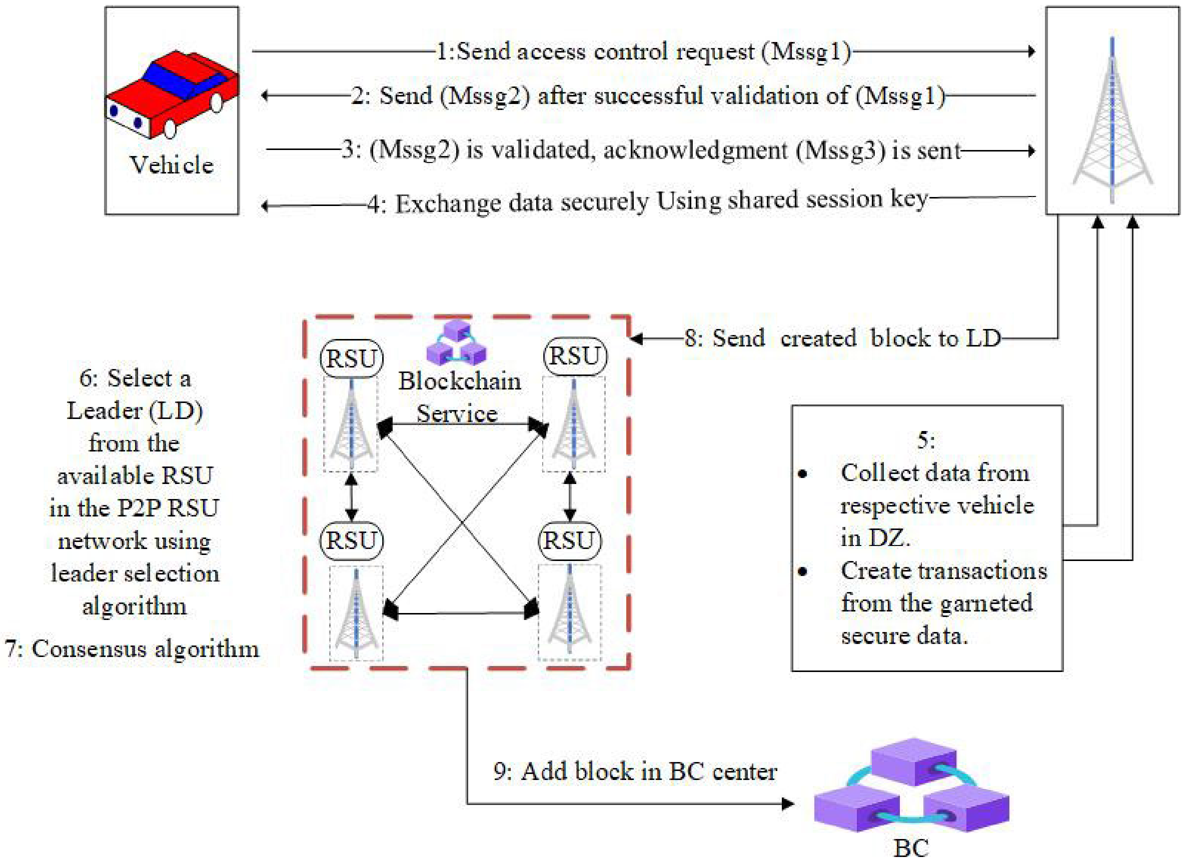


FIGURE 4. System architecture.

only V_i process the secret key SK_{V_i} SK_{v_i}. Without the knowledge of the private key of RSU, an attacker cannot generate a correct and valid D- Ver.

- Vehicle impersonation attack: an attacker could present himself as a legal vehicle to obtain benefits, causing confusion and misleading IoV members. Through this identity attack, the attacker successfully speculation about a genuine credential and uses it to log in to the IoV network. BSDCE-IoV scheme uses the digital signature ($Dsign_{V_n}$) to authenticate the real data sender. $Dsign_{V_n}$ is generated using the private key of V_n (SK_{V_n}) that is known only by the owner. $Dsign_{V_n}$is verified by checking $Dsign_{V_n}.G = AV_n + h_1 * PK_{V_n}$. If both sides of the equation are equal, then the sender of the data is as it pretends to be, otherwise, an impersonation attack will be determined. Verification can be done because all data is public or received in $Mssg_1$ except SK_{V_n}.
- Impersonation attack of RSU: - the attacker impersonates RSU to obtain confidential information or sabotage the IoV network. To check the authenticity of the RSU_j by the vehicle V_n, the certificate of the RSU is verified through the equation $Certif_{RSU_j}.G = Pub_{RSU_j} + h(RID_{RSU_j} \parallel Pub_{RSU_j} \parallel Pub_{CR_i}) * PK_{CR_i}) \pmod p$. Verification of the equality of both sides is possible because all data is public except the private key of RSU_j.
- Mutual authentication: - The proposed algorithm ensures the mutual authentication of the entities involved in the process. BSDCE-IoV uses digital signature and certificates to authenticate both vehicles and RSU. The private/ public keys of the ECC algorithm are the base of the mutual authentication.
- Session key security: - The generation of the session key is accomplished by using the approved (Diffie-Hillman) algorithm. Session key exchange using D-H is protected by the D-Ver based on the use of unique MK_{RSU}.
- Sybil Attack: - is a type of attack on a network in which an attacker creates a large number of pseudonymous identities and uses them to gain a significant influence. By using private-public key pair of every vehicle, RSU, CR, and RA, an attacker will not be able to have more than one authenticated connection to the system.
- GPS attack:- is when a Vehicle alters data so that a device appears in a different location or time zone. An attacker would position a broadcast antenna and point it at the target's GPS receiver antenna to interfere with GPS signals. Use blocking antennas: Blocking antennas can

TABLE 4. Attributes of functionality and security comparison.

Attribute	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[Our]
AFS_1	✓	✓	✓	✓	✓	✓	✓	✓
AFS_2	X	✓	✓	✓	✓	✓	X	✓
AFS_3	✓	✓	✓	✓	✓	✓	✓	✓
AFS_4	✓	X	✓	X	✓	X	X	✓
AFS_5	✓	X	✓	✓	✓	✓	✓	✓
AFS_6	X	X	✓	✓	✓	✓	✓	✓
AFS_7	✓	X	X	✓	✓	X	X	✓
AFS_8	X	X	X	X	X	X	X	✓
AFS_9	X	✓	X	X	X	X	X	✓
AFS_{10}	X	X	X	X	✓	✓	✓	✓
AFS_{11}	X	X	X	X	X	✓	✓	✓

AFS_1: "Replay Attack"; AFS_2: "Man-in-the-Middle Attack"; AFS_3: "Impersonation Attack Vehicle"; AFS_4: "Impersonation attack of RSU"; AFS_5: "Mutual authentication"; AFS_6: "Session key security"; AFS_7: "Sybil Attack"; AFS_8: "GPS attack"; AFS_9: "Physical Vehicle Capture Attack"; AFS_{10}: "blockchain based solution"; AFS_{11}: "security verification using AVISPA OR Seyther Tools";

protect against interference and jamming and reduce the danger of spoofing signals. A robust clock (Synchronization) to define accurately the transmission time and the reception time of the message between two Vs or V-2-RSU carrying GPS information. The calculation of the time difference indicates the location of V, followed by comparing this information to GPS data. To overcome the possibility of tricking the time information, the distances between V and two RSUs are calculated. The intersection of results with GPS information can reveal the attacker-V.

- Physical Vehicle Capture Attack: - Protected by using the unique private-public key for every vehicle. So, the physical capture will harm just the security of one vehicle (capture one).

B. FORMAL SECURITY ANALYSIS UNDER RoR ORACLE MODEL

In this section, the proposed BSDCE-IoV is formally analyzed using the Real-or-Random (RoR) oracle model to validate the secure key sharing among V_n and RSU [50]. (RoR) oracle model based on semantic security notion is considered in Theorem 1 for security proving. It is worth noting that in this model cryptographic one-way hash function h(.) is simulated as a random oracle (RO), for instance, hash digest Hd. The malicious attacker is permitted to execute the following set of queries:

Execution ($\mu_{V_n}^{s1}$, μ_{RSU}^{s2}): The adversary A utilizes the execution query to forge the exchange contents between legal members V_n and RSU

Vehicle_seize ($\mu_{V_n}^{s1}$): A utilizes the Vehicle_seize query to extract the secret factors from the memory of the seized vehicle V_n.

Corrupt(μ^s): A uses the corrupt query to expose the previous session keys that were established and shared secretly between μs and the corresponding partner.

Test (μ^s): A utilizes the Test query to verify the authenticity of the exposed session key with the help of an unbiased coin c flipped randomly. The demonstration of the (RoR) oracle model employs the understated elements:

Participants: The mutual authentication considers two participating entities, i.e. vehicle Vn and RSU. We assume that $\mu_{V_n}^{s1}$ and μ_{RSU}^{s2} characterize s_1 and s_2 as the two instances for Vn and RSU, respectively. We delineate the respective instances as "random oracles".

Accepted state: The exchanged messages are assumed to be ordered in a sequence, forming the session-based identification *sid* regarding μ^s in the current session.

Partnering: The instances μ^{s_1} and μ^{s_2} are said to be partners, in case both of these meet the understated criteria:

- The instances μ^{s_1} and μ^{s_2} should be in accept state.
- The instances μ^{s_1} and μ^{s_2} need to authenticate one another on a mutual basis.
- The instances μ^{s_1} and μ^{s_2} behave as partners for one another with a common session identity *sid*.

Freshness: Either of the instances μ^{s_1} or μ^{s_2} is regarded as fresh in case the mutually agreed session key $SKey_{V_n-RSU}$ or $SKey_{RSU-V_n}$ between V and RSU is not exposed to the attacker with the execution of Corrupt (μ^s) query.

We employ the following definition of semantic security for theorem 1 validation.

Definition 1 ("Semantic Security"): The $Adv_A^{BSDCE-IoV}$ (t_p) depicts the adversary A's advantage to compromise the semantic security of the contributed BSDCE-IoV in polynomial time tp and recover the session key $SKey_{V_n-RSU}$ ($= SKey_{RSU-V_n}$) as established between V and RSU, Thus

$$Adv_A^{BSDCE-IoV}(t_p) = |2.Pr[cb = gb] - 1| \quad (1)$$

cb and *gb* represent the correct and guessed bits, respectively.

Definition 2 ("Elliptic Curve Discrete Logarithm Problem (ECDLP)"): We consider an elliptic curve E_q(a, b) having two points Q, R $\in E_q$(a, b), find an integer

y such that $R = y.\ \varrho$, where $y \in Z_q^* = \{1, 2, \ldots, p-1\}$ is termed as the discrete logarithm with the base ϱ and k. ϱ indicates the scalar point multiplication.

Theorem 1: We assume an adversary A, executing the protocol in polynomial time t_p, attempts to guess the established session key between the participants V_n and RSU as regards a particular session of the BSDCE-IoV model. We also assume that qhd, $|hash_f|$ and Adv_A^{EC-DLP} (t_p) signify the number of hash function queries, the range margin for cryptographic collision resistant one-way hash digest function h(.), and the benefit for compromising the Elliptic Curve Discrete Logarithm Problem (ECDLP) as given in definition 2, respectively.

$$Adv_A^{BSDCE-IoV}(t_p) \leq \frac{q_{hd}^2}{|hash_f|} + Adv_A^{ECD-DLP}(t_p) \quad (2)$$

Proof: The proof employs a sequence of three games for verifying the security attributes of the BSDCE-IoV scheme. The adversary may launch three games, i.e., $Game_k^A$, where $(0 \leq k \leq 2)$ holds. The $Succ_{Game_k}^A$ indicates an event for which the attacker A attempts to guess a random bit c correctly for a particular game $Game_k^A$. Thus the chances of success or winning probability of the attacker for game Game_k^A may be denoted as $\text{Adv}_{A,Game_k}^{BSDCE-IoV} = \Pr[\text{Succ}_{Game_k}^A]$. The illustration of each game is given below:

Game_0^A This game is played by the attacker in realistic terms to break the security of BSDCE-IoV. To serve the purpose, the attacker chooses a bit c on a random basis for initiating the game Game_0^A under (RoR) oracle model. The semantic security by definition 1 may be shown as:

$$Adv_A^{BSDCE-IoV}(t_p) = |2\, Adv_{A,Game_0}^{BSDCE-IoV}(t_p) - 1| \quad (3)$$

$Game_1^A$ By employing this game, an attacker eavesdrop the messages $\text{Mssg}_1 = \{\text{RID}_{V_n}, \text{Certif}_{V_n}, \text{A}_{V_n}, \text{Dsign}_{V_n}, \text{TS}_1\}$, $\text{Mssg}_2 = \{\text{RID}_{RSU}, \text{Certif}_{RSU}, \text{B}_{RSU}, \text{SKey-Ver}_{RSU-V}, \text{TS}_2\}$, and $\text{Mssg}_3 = \{\text{ACK}_{V-RSU}, \text{TS}_3\}$ as exchanged between the Vn and RSU. Next, it runs an Execution query to attempt to extract the session key SKey_{V_n-RSU} ($= \text{SKey}_{RSU-V_n}$) by employing the intercepted communication messages on an open channel. The attacker may execute Reveal as well as Test queries for verifying the correctness of the recovered session key, or otherwise, it could merely be a random key. For recovering the session key $\text{SKey}_{V_n-RSU} = \text{h}\ (\text{RID}_{V_n} \parallel \text{RID}_{RSU} \parallel \text{DHKey}_{V-RSU} \parallel \text{PK}_{V_n} \parallel \text{PK}_{RSU})$, it requires to extract not only short term parameters, i.e. R_1, R2 to compute $\text{DHKey}_{V_n-RSU} = \text{R}_1'.\text{B}_{RSU} = (\text{R}_1' * \text{R}_2').\text{G}$ and the corresponding session key SKey_{V_n-RSU}, but also need long term parameters such as MK_{CR_i} and SKV_n to compute the corresponding certificates and the related parameters including R_1', R_2'. All of these parameters are employed in the construction of the session key by taking hash function h(.), and thus cannot be recovered in polynomial time tp. Hence mere recovery of any of these parameters may not help the attacker to compute the session key SKey_{V_n-RSU} ($= \text{SKey}_{RSU-V_n}$). Thus the games $Game_0^A$ and $Game_1^A$ remain indistinguishable in the case of eavesdropping threat.

$$Adv_{A,Game_0}^{BSDCE-IoV} = Adv_{A,Game_1}^{BSDCE-IoV} \quad (4)$$

Game_2^A By using this game, the attacker simulates an active attack using $hash_f$ queries and attempts to solve the EC-DLP problem to compute the session key $\text{SKey}_{V_n-RSU} = \text{h}(\text{RID}_{V_n} \parallel \text{RID}_{RSU} \parallel \text{DHKey}_{V-RSU} \parallel \text{PK}_{V_n} \parallel \text{PK}_{RSU})$.

However, as we stated earlier that for this purpose it needs to get access to short-term parameters, i.e. R_1, R_2 as well as long-term parameters such as $MK_{CR_i} and SK_{V_n}$ to compute the parameters $DHKey_{(V_n-RSU} = R_1'.B_{RSU} = (R_1' * R_2')$. G and the ultimate session key $SKey_{V_n-RSU}$. It is worth mentioning that the secret $DHKey_{v-RSU}$ in the constructed session key $SKey_{V_n-RSU} = SKey_{RSU-V_n}$ is protected under collision-resistant, cryptographic one-way hash function h(.). By intercepting the messages on the public channel $Mssg_1 = \{RID_{V_n}, Certif_{V_n}, A_{V_n}, Dsign_{V_n}, TS_1\}$, $Mssg_2 = \{RID_{RSU}, Certif_{RSU}, B_{RSU}, SKey - Ver_{RSU-V_n}, TS_2\}$. and $Mssg_3 = ACK_{V_n-RSU}$ it may not compute the secret $DHKey_{v-RSU}$ or the corresponding certificates such a $Certif_{RSU_j}$ or $Certif_{V_n}$. Moreover, to recover the $\{R_1', R_2'\}$ parameters from the intercepted A_{V_n} and B_{RSU}, the adversary need to break the ECDLP problem and solve $hash_f$, then it may compute the session key. We can witness that both of the games $Game_1^A$ and $Game_2^A$ remain indistinguishable in the absence of simulation for $hash_f$ and ECDLP. Thus, by employing the birthday paradox, we get the following advantage to solve ECDLP:

$$|Adv_{A,Game_1}^{BSDCE-IoV} = Adv_{A,Game_2}^{BSDCE-IoV}| \leq \frac{q_{hd}^2}{2|hash_d|} + Adv_A^{ECDLP}(t_p) \quad (5)$$

Now the adversary attempts to win the game by guessing the bit and computing the correct session key as given below: $Adv_{A,Game_2}^{BSDCE-IoV} = \frac{1}{2}$

Referring to equation (1)

$$\frac{1}{2}.Adv_A^{BSDCE-IoV} = |Adv_{A,Game_0}^{BSDCE-IoV} - \frac{1}{2}|$$

Using the equations (3), (4), and (5) and triangular inequality, we have

$$\begin{aligned}\frac{1}{2}.Adv_A^{BSDCE-IoV} &= |Adv_{A,Game_0}^{BSDCE-IoV}(t_p) - |\text{Adv}_{A,Game_2}^{BSDCE-IoV}| \\ &= |Adv_{A,Game_1}^{BSDCE-IoV}(t_p) - |\text{Adv}_{A,Game_2}^{BSDCE-IoV}| \\ &\leq \frac{q_{hd}^2}{2|hash_d|} + Adv_A^{ECDLP}(t_p) \end{aligned} \quad (6)$$

Having used equation (6), we derive the following equation:

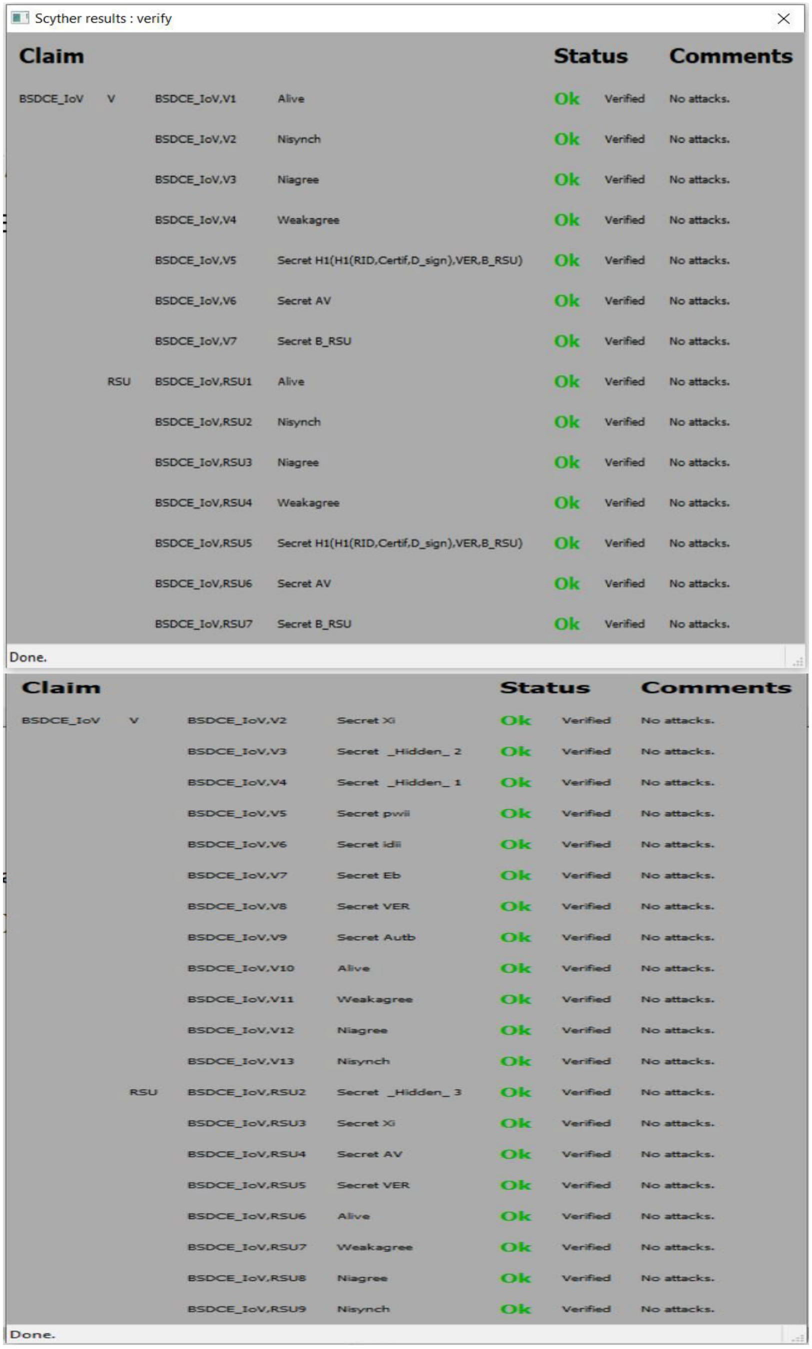
$$Adv_A^{ECDLP}(t_p) \leq \frac{q_{hd}^2}{2|hash_d|} + 2Adv_A^{ECDLP}(t_p)$$

C. FORMAL SECURITY VERIFICATION USING SCYTHER TOOL

Scyther is an automated security verification tool that can characterize protocols, yielding a finite representation of all possible protocol behaviors. It is a way to formally verify the security level of a protocol by analyzing it and discovering the existing weakness based on the Dolev-Yao threat model. Scyther is a standard verification protocol, especially for verifying authentication, and it is used more than other tools such as AVISPA and Proverif.

Scyther displays whether your supposed information privacy is preserved or not through the security schemes execution phase. This is because the attack opportunity usually happens in the scheme execution or description phases. The schemes should be written in the Security Protocol Description Language (SPDL), which defines protocols, encryption, decryption, signature, and sending/receiving events. SPDL includes steps, the verification claim and the automatic claim [51].

The simulation results using Scyther demonstrate that BSDCE-IoV is safe against adversary attacks on data privacy during the scheme execution phase, as depicted in Figure 5. BSDCE-IoV satisfies all security claims of the protocol by investigating and validating the secrecy of the proposed authentication.



Scyther results : verify

Claim				Status		Comments
BSDCE_IoV	V	BSDCE_IoV,V1	Alive	Ok	Verified	No attacks.
		BSDCE_IoV,V2	Nisynch	Ok	Verified	No attacks.
		BSDCE_IoV,V3	Niagree	Ok	Verified	No attacks.
		BSDCE_IoV,V4	Weakagree	Ok	Verified	No attacks.
		BSDCE_IoV,V5	Secret H1(H1(RID,Certif,D_sign),VER,B_RSU)	Ok	Verified	No attacks.
		BSDCE_IoV,V6	Secret AV	Ok	Verified	No attacks.
		BSDCE_IoV,V7	Secret B_RSU	Ok	Verified	No attacks.
	RSU	BSDCE_IoV,RSU1	Alive	Ok	Verified	No attacks.
		BSDCE_IoV,RSU2	Nisynch	Ok	Verified	No attacks.
		BSDCE_IoV,RSU3	Niagree	Ok	Verified	No attacks.
		BSDCE_IoV,RSU4	Weakagree	Ok	Verified	No attacks.
		BSDCE_IoV,RSU5	Secret H1(H1(RID,Certif,D_sign),VER,B_RSU)	Ok	Verified	No attacks.
		BSDCE_IoV,RSU6	Secret AV	Ok	Verified	No attacks.
		BSDCE_IoV,RSU7	Secret B_RSU	Ok	Verified	No attacks.

Done.

Claim				Status		Comments
BSDCE_IoV	V	BSDCE_IoV,V2	Secret Xi	Ok	Verified	No attacks.
		BSDCE_IoV,V3	Secret _Hidden_ 2	Ok	Verified	No attacks.
		BSDCE_IoV,V4	Secret _Hidden_ 1	Ok	Verified	No attacks.
		BSDCE_IoV,V5	Secret pwii	Ok	Verified	No attacks.
		BSDCE_IoV,V6	Secret idii	Ok	Verified	No attacks.
		BSDCE_IoV,V7	Secret Eb	Ok	Verified	No attacks.
		BSDCE_IoV,V8	Secret VER	Ok	Verified	No attacks.
		BSDCE_IoV,V9	Secret Autb	Ok	Verified	No attacks.
		BSDCE_IoV,V10	Alive	Ok	Verified	No attacks.
		BSDCE_IoV,V11	Weakagree	Ok	Verified	No attacks.
		BSDCE_IoV,V12	Niagree	Ok	Verified	No attacks.
		BSDCE_IoV,V13	Nisynch	Ok	Verified	No attacks.
	RSU	BSDCE_IoV,RSU2	Secret _Hidden_ 3	Ok	Verified	No attacks.
		BSDCE_IoV,RSU3	Secret Xi	Ok	Verified	No attacks.
		BSDCE_IoV,RSU4	Secret AV	Ok	Verified	No attacks.
		BSDCE_IoV,RSU5	Secret VER	Ok	Verified	No attacks.
		BSDCE_IoV,RSU6	Alive	Ok	Verified	No attacks.
		BSDCE_IoV,RSU7	Weakagree	Ok	Verified	No attacks.
		BSDCE_IoV,RSU8	Niagree	Ok	Verified	No attacks.
		BSDCE_IoV,RSU9	Nisynch	Ok	Verified	No attacks.

Done.

FIGURE 5. Verification claim and verification auto claim.

VI. MIRACL EXPERIMENTAL RESULTS

The proposed BSDCE-IoV execution time cost has been measured by the accepted ''multi-precision Integer and Rational Arithmetic Cryptographic Library'' (MIRACL) through a variety of existing cryptographic primitives [52]. Cryptographers have broadly recognized MIRACL as the best open-source SDK standard for ECC, which is a ''C/C++ based programming software library''.

HP Elite/Book (8460P), with its 2.7 GHz CPU-Processor (Core i7) and 4 Gigabytes RAM-memory, is used as an RSU station in our experimental implementation based on the MIRACL library. As well, the Pi3/B+ card, and Cortex-A53-ARMv8 (64 bit)-SoC @ are used to reproduce the vehicle with its a 1.4 GHz CPU-processor, and 1 Gigabyte LPDDR2 SDRAM.

Table 5 lists the simulation results for both RSU and vehicles. While, Figure 6 provides the execution time for the proposed BSDCE-IoV and selected recent schemes in related fields [35], [36], [37], [38], [39], [40], and [41]. The cost function of a single authentication cycle of the BSDCE-IoV

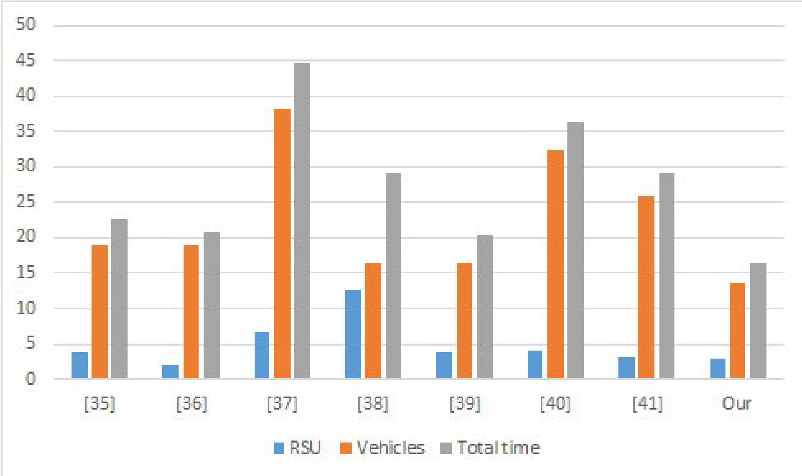


FIGURE 6. Comparison of computational overhead.

TABLE 5. MIRACL execution time (ms).

Operation	RSU	Vehicle
T_B: Bilinear pairing	4.038	12.52
T_M: Point multiplication	0.926	4.107
T_A: Point Addition	0.006	0.018
T_R: Random number Generation	0.118	1.185
T_H: One-way Hash	0.004	0.006

is $10T_H + 2T_R + 6T_M + 3T_A$, with an approximate time of 16.484 ms. The proposed algorithm outperforms all the other schemes in terms of total execution time, added to its improved security.

VII. COMPARATIVE ANALYSIS

A comparison of the proposed BSDCE-IoV with schemes [35], [36], [37], [38], [39], [40], and [41] in terms of security, functionality characteristics, and computation costs in this section.

A. COMMUNICATION COST

The communication cost of the proposed scheme is analyzed by computing the size of different exchanged messages during mutual-authentication phases. Based on the supposition that a number of bits of 32, 256, 320 (160+160), 160, and 160 are used in order for "timestamp", "SHA-256", "elliptic curve point multiplication", "random integer", and "identity" functions. The total costs of messages $Mssg_1 = \{RID_{V_n}, Certif_{V_n}, A_{V_n}, Dsign_{V_n}, TS_1\}$, $Mssg_2 = \{RID_{RSU}, Certif_{RSU}, B_{RSU}, SKey\text{-}Ver_{RSU-V}, TS_2\}$, and $Mssg_3 = \{ACK_{V-RSU}, TS_3\}$ are 928, 1024, and 288 bits, respectively. The comparison of BSDCE-IoV with the other schemes is depicted in Table 7. Our proposed scheme outperforms the schemes [35], [36], [37], [38], [39], [40], and [41] by a gain of 27%, 13%, 29%, 12%, 13%, 23%, and 16%, respectively. As a result, compared to other schemes, BSDCE-IoV has a lower communication cost.

B. COMPUTATION COSTS COMPARISON

We suppose that T_H, T_M, T_A, T_B, and T_R are times needed respectively for, "one-way hash function", "point multiplication", "point addition", "bilinear pairing", and "random number generation". The computing cost for a vehicle V_i in the proposed BSDCE-IoV is $6T_H+T_R+3T_M+T_A$, while the computation cost for an RSU_j is $4T_H+T_R+3T_M+2T_A$. Using MIRACL, we apply the experimental findings from Table 4 to a variety of cryptographic primitives. For comparing the computation times of BSDCE-IoV and related schemes, the time-cost of primitive functions in Table 6 is used. BSDCE-IoV computation cost has a gain of respectively, 120%, 77%, 38%, 26%, 25%, 78%, and 85% compared to the computation costs of schemes [35], [36], [37], [38], [39], [40], and [41]. In addition, BSDCE-IoV offers more functionality capabilities and better security than the earlier schemes.

C. SECURITY AND FUNCTIONALITY FEATURES COMPARISON

Table 4 presents a comparison of the "functionality and security attributes" (AFS_1-AFS_{11}) of BSDCE-IoV and other related schemes. BSDCE-IoV has better performances compared to the selected schemes in terms of security and functionality, and it also provides additional functionality features.

D. DISCUSSION

During the system initialization phase of the IoV system, the RA is responsible for registration and admission to CRs. The choice of IoV system security parameters is also within the responsibility of the RA. After that, RSU_j and vehicles (V_i) are registered by their corresponding CR. It is important to note that the BSDCE-IoV registration process is a one-time procedure and is accomplished in a decentralized manner.

The proposed access control is used to establish session keys to secure V2RSU and V2V communication processes.

TABLE 6. Computation costs comparison.

Reference	Year	Type	RSU	Vehicle	Total time (ms)
[35]	2021	IoV	$3T_H + T_R + 4T_M = 3.834$	$6T_H + 2T_R + 4T_M = 18.834$	22.668
[36]	2022	IoV	$T_H + T_R + 2T_M = 1.974$	$2T_H + 2T_R + 4T_M + 1T_A = 18.828$	20.802
[37]	2022	IoV	$2T_H + T_R + 7T_M = 6.608$	$T_H + T_R + 9T_M = 38.154$	44.762
[38]	2019	IoV,IoT	$5T_H + 2T_B + 5T_M + 3T_A = 12.744$	$5T_H + 4T_M = 16.458$	29.202
[39]	2020	IoV	$6T_H + 4T_M + T_A = 3.734$	$5T_H + 4T_M + T_A = 16.476$	20.21
[40]	2021	IoV	$7T_H + 2T_R + 4T_M = 3.968$	$8T_H + 3T_R + 7T_M = 32.352$	36.32
[41]	2022	IoV	$8T_H + 3T_R + 3T_M = 3.164$	$11T_H + T_R + 6T_M = 25.893$	29.057
[Our]	2022	IoV	$4T_H + T_R + 3T_M + 2T_A = 2.924$	$6T_H + T_R + 3T_M + T_A = 13.56$	16.484

TABLE 7. Communication cost.

Scheme	No. of mssg	Total cost (in bits)	Gain
[35]	2	2848	27%
[36]	2	2528	13%
[37]	2	2880	29%
[38]	2	2496	12%
[39]	2	2528	13%
[40]	4	2752	23%
[41]	2	2592	16%
Our	3	2240	-

Additionally, the BSDCE-IoV data collection and transmission strategy enable the recording of all communicating data among CR, RSU, and vehicles. This transaction recording is then used for the creation of private blocks by RSU, followed by the verification and addition of blocks by an RSU_j as the leader in the P2P RSU network in the blockchain.

Finally, the BSDCE-IoV scheme proves its decentralized nature. However, for a realistic deployment of the IoV environment, a BC simulation is necessary as part of our plan.

VIII. CONCLUSION

In this research, the BSDCE-IoV as a secure data exchange method for a 5G-enabled IoV environment has been introduced. BSDCE-IoV presents an original blockchain-based authenticated key agreement scheme for IoV environment. In addition to supporting a solid strategy for the control access between RSUs and vehicles, it offers safe transactions among the vehicles, RSUs, and control rooms in the DZ, and is added to the blockchain network via the corresponding RSU.

A created block is sent to the RSU-leader node, which is selected from the group of RSUs present in the P2P RSU network. The leader performs verification, validation, and addition of the block in the blockchain network, assisted by the blockchain center by using the known Practical Byzantine Fault Tolerance consensus algorithm. It has been demonstrated that BSDCE-IoV is resistant to various possible blockchain attacks. BSDCE-IoV performance analysis is also carried out.

BSDCE-IoV proves its capability to defend against classical attacks such as replay, impersonation (for both RSU and vehicles), Sybil, GPS, Man-in-the-middle, and physical vehicle capture attacks and ensures anonymity and untraceability for the vehicles. A complete informal analysis of all potential attacks combined with formal analysis and performance validation shows that the proposed BSDCE-IoV solution achieves the required level of security with minimal computational and communication overheads. in the future, further studies can be focused on the optimization and implementation of an even more efficient, flexible, and practical vehicular network.

REFERENCES

[1] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions," *Secur. Commun. Netw.*, vol. 2022, Oct. 2022, Art. no. 1131479.

[2] A. A. Almohammedi, N. K. Noordin, A. Sali, F. Hashim, and M. Balfaqih, "An adaptive multi-channel assignment and coordination scheme for IEEE 802.11 P/1609.4 in vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 2781–2802, 2017.

[3] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, 2021.

[4] M. A. Shawky, M. Usman, M. A. Imran, Q. H. Abbasi, S. Ansari, and A. Taha, "Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100547.

[5] F. Z. Alden, S. Hassan, A. Habbal, and X. Wei, "An adaptive social-aware device-to-device communication mechanism for wireless networks," *Ad Hoc Netw.*, vol. 137, Dec. 2022, Art. no. 102955.

[6] N. M. Elfatih, M. K. Hasan, Z. Kamal, D. Gupta, R. A. Saeed, E. S. Ali, and M. S. Hosain, "Internet of Vehicle's resource management in 5G networks using AI technologies: Current status and trends," *IET Commun.*, vol. 16, no. 5, pp. 400–420, Mar. 2022.

[7] G. K. Ijemaru, L. M. Ang, and K. P. Seng, "Transformation from IoT to IoV for waste management in smart cities," *J. Netw. Comput. Appl.*, vol. 204, Aug. 2022, Art. no. 103393.

[8] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, and H. Ma, "Federated learning-based collaborative authentication protocol for shared data in social IoV," *IEEE Sensors J.*, vol. 22, no. 7, pp. 7385–7398, Apr. 2022.

[9] M. Alabadi, A. Habbal, and X. Wei, "Industrial Internet of Things: Requirements, architecture, challenges, and future research directions," *IEEE Access*, vol. 10, pp. 66374–66400, 2022.

[10] S. A. Chaudhry, A. Irshad, J. Nebhen, A. K. Bashir, N. Moustafa, Y. D. Al-Otaibi, and Y. B. Zikria, "An anonymous device to device access control based on secure certificate for Internet of Medical Things systems," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103322, doi: 10.1016/j.scs.2021.103322.

[11] S. Y. A. Zaidi, M. A. Shah, H. A. Khattak, C. Maple, H. T. Rauf, A. M. El-Sherbeeny, and M. A. El-Meligy, "An attribute-based access control for IoT using blockchain and smart contracts," *Sustainability*, vol. 13, no. 19, p. 10556, Sep. 2021.

[12] S. Mohamed, M. Çakmak, and Z. Albayrak, "Security classification of smart devices connected to LTE network," in *Proc. 6th Int. Conf. Smart City Appl.* Cham, Switzerland: Springer, 2022, pp. 1125–1131.

[13] A. Habbal, S. I. Goudar, and S. Hassan, "A context-aware radio access technology selection mechanism in 5G mobile network for smart city applications," *J. Netw. Comput. Appl.*, vol. 135, pp. 97–107, Jun. 2019.

[14] S. Hakak, T. R. Gadekallu, P. K. R. Maddikunta, S. P. Ramu, M. Pari-Mala, C. De Alwis, and M. Liyanage, "Autonomous vehicles in 5G and beyond: A survey," *Veh. Commun.*, vol. 39, Feb. 2022, Art. no. 100551.

[15] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: A pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," *IEEE Syst. J.*, vol. 16, no. 1, pp. 309–316, Mar. 2022, doi: 10.1109/JSYST.2020.3036425.

[16] I. Darman, M. K. Mahmood, S. A. Chaudhry, S. A. Khan, and H. Lim, "Designing an enhanced user authenticated key management scheme for 6G-based industrial applications," *IEEE Access*, vol. 10, pp. 92774–92787, 2022.

[17] E. Benalia, S. Bitam, and A. Mellouk, "Data dissemination for Internet of Vehicle based on 5G communications: A survey," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 5, p. e3881, May 2020.

[18] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[19] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2002, pp. 337–351.

[20] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proc. IEEE*, vol. 108, no. 2, pp. 357–372, Feb. 2020.

[21] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, "Three-factor authentication protocol using physical unclonable function for IoV," *Comput. Commun.*, vol. 173, pp. 45–55, May 2021.

[22] I. Ahmim, N. Ghoualmi-Zine, A. Ahmim, and M. Ahmim, "Security analysis on 'three-factor authentication protocol using physical unclonable function for IoV,'" *Int. J. Inf. Secur.*, vol. 21, no. 5, pp. 1–8, 2022.

[23] M. Zhang, J. Zhou, G. Zhang, M. Zou, and M. Chen, "EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles," *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102161.

[24] S. Bojjagani, Y. P. Reddy, T. Anuradha, P. V. Rao, B. R. Reddy, and K. M. Khan, "Secure authentication and key management protocol for deployment of Internet of Vehicles (IoV) concerning intelligent transport systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 24698–24713, Sep. 2022.

[25] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.

[26] M. S. Eddine, M. A. Ferrag, O. Friha, and L. Maglaras, "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled Internet of Vehicles," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102802.

[27] G. Xu, H. Bai, J. Xing, T. Luo, N. N. Xiong, X. Cheng, S. Liu, and X. Zheng, "SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of Vehicles," *J. Parallel Distrib. Comput.*, vol. 164, pp. 1–11, Jun. 2022.

[28] H. Chai, S. Leng, J. He, K. Zhang, and B. Cheng, "CyberChain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4620–4631, May 2022.

[29] M. Shen, H. Lu, F. Wang, H. Liu, and L. Zhu, "Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12250–12263, Nov. 2022.

[30] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. H. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of Vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[31] M. A. Saleem, K. Mahmood, and S. Kumari, "Comments on 'AKM-IoV: Authenticated key management protocol in fog computing-based Internet of Vehicles deployment,'" *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4671–4675, May 2020.

[32] N. Xi, W. Li, L. Jing, and J. Ma, "ZAMA: A ZKP-based anonymous mutual authentication scheme for the IoV," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22903–22913, Nov. 2022.

[33] D. S. Gupta, A. Karati, W. Saad, and D. B. da Costa, "Quantum-defended blockchain-assisted data authentication protocol for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 3255–3266, Mar. 2022.

[34] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, "Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET," *Future Internet*, vol. 12, no. 4, p. 63, Apr. 2020.

[35] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14248–14257, Sep. 2021.

[36] L. Shen, L. Wang, K. Zhang, J. Li, and K. Chen, "An efficient conditional privacy-preserving authentication scheme with scalable revocation for VANETs," *J. Syst. Archit.*, vol. 133, Dec. 2022, Art. no. 102764.

[37] H. J. Nath and H. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in VANET," *Comput. Commun.*, vol. 192, pp. 357–372, Aug. 2022.

[38] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Syst. J.*, vol. 14, no. 1, pp. 560–571, Mar. 2020.

[39] J. Wang, L. Wu, K.-K.-R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[40] 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.*, Jun. 2021, pp. 1–6.

[41] 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. 8, no. 18, pp. 14248–14257, Jan. 2022.

[42] S. Nakamoto, "BitCoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, vol. 10, p. 21260, Oct. 2008.

[43] R. Gupta, S. Tanwar, and N. Kumar, "B-IoMV: Blockchain-based onion routing protocol for D2D communication in an IoMV environment beyond 5G," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100401.

[44] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," University of Waterloo, Waterloo, ON, Canada, Tech. Rep., 1999. [Online]. Available: https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf

[45] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, pp. 955–967, Jan. 2019.

[46] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10792–10806, Jul. 2021.

[47] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[48] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Jun. 2018.

[49] A. Kapitonov, I. Berman, S. Lonshakov, and A. Krupenkin, "Blockchain based protocol for economical communication in industry 4.0," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 41–44.

[50] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *IEE Proc.-Inf. Secur.*, vol. 153, no. 1, pp. 27–39, 2006.

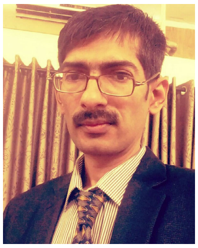
[51] C. J. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols: Tool paper," in *Proc. Int. Conf. Comput. Aided Verification*. Cham, Switzerland: Springer, 2008, pp. 414–418.

[52] (2020). *Miracl Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library*. [Online]. Available: https://github.com/miracl/MIRACL/

SULAIMAN M. KARIM received the bachelor's degree in computer science from the College of Computer Science and Mathematics, Tikrit University, Iraq, in 2015, and the M.S. degree in computer engineering from Erciyes University, Turkey, in 2019. He is currently pursuing the Ph.D. degree with Karabük Üniversitesi. His research interests include the IoV security, clustering, WSN, and blockchain.

ADIB HABBAL (Senior Member, IEEE) received the Ph.D. degree in computer science (specializing in networked computing) from Universiti Utara Malaysia (UUM), Malaysia. He is currently a Professor (Associate) of computer engineering and the Founding Head of the Innovative Networked Systems (INETs) Research Group, Karabük Üniversitesi, Turkey. Before joining Karabük Üniversitesi, in 2019, he was a Senior Lecturer with Universiti Utara Malaysia, for ten years; and the Head of the InterNetWorks Research Platform for three years. His research projects has funded by several organizations, including IEEE R10, IEEE Malaysia Section, Internet Society, the Chinese Academy of Science, Malaysian Ministry of Higher Education, UUM, and others. He has authored/coauthored 100 refereed technical publications in journals and conference proceedings in the areas of future internet and wireless networks. His research interests include future internet protocols and architecture, next generation mobile networks, WEB3, blockchain technology, and digital trust. He served as an IEEE UUM Student Branch Founding Counselor and an Executive Council Member for the Internet Society Malaysia Chapter. He has received a number of international recognitions for his outstanding educational and research activities, including the UUM Excellent Service Award, in 2010, the UUM Best Research Award, in 2014, and the UUM-SOC Prolific Writer Award, in 2016. He was a recipient of the Internet Society Fellowship to the Internet Engineering Task Force (IETF), the IEEE Malaysia Section Best Volunteer Award, and the Asia–Pacific Advanced Network (APAN) Fellow to APAN35. His professional experience includes being a speaker at a number of renowned research conferences and technical meetings, such as ACM SIGCOMM, APAN, APRICOT, IEEE, and internet2; an editor of top tier and refereed journals and a technical program committee for international conferences on computing networks; and an examiner of postgraduate scholars in his research areas.

SHEHZAD ASHRAF CHAUDHRY received the master's and Ph.D. degrees (Hons.). Currently, he is an Associate Professor of cybersecurity engineering with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates. Before this, he served with Istanbul Gelisim University, Turkey; the University of Sialkot, Pakistan; and International Islamic University, Islamabad, Pakistan. He has also supervised more than 40 graduate students in their research. Working in the field of information and communication security, he has published extensively in prestigious venues, such as *IEEE Communications Standards Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON RELIABILITY, *ACM Transactions on Internet Technology*, *Sustainable Cities and Society* (Elsevier), *FGCS*, *IJEPES*, *Computer Networks*, and *Digital Communications and Networks*. He occasionally writes on issues of higher education in Pakistan. Over 150 publications and with an H-index of 41, I-10 index of 95, and accumulate impact factor of more than 390, he has published more than 127 SCI/E indexed manuscripts and his works have been cited more than 4500 times. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystems, and next generation networks. He was awarded the Gold Medal for achieving maximum distinction of 4/4 CGPA in his master's degree. In 2018, considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. For the consecutive three years (i.e., 2020, 2021, and 2022), he is being listed among top 2% computer scientists across the world in Stanford University's report.



AZEEM IRSHAD received the master's degree from Arid Agriculture University, Rawalpindi, Pakistan, and the Ph.D. degree from International Islamic University, Islamabad, Pakistan. He has authored more than 90 international journal articles and conference publications, including 50 SCI-E journal publications. His research work has been cited over 1400 times with an H-index of 16 and I-10-index of 28. Recently, he has co-edited a book titled *IoT and Smart Devices for Sustainable Environment* (Springer). His research interests include strengthening of authenticated key agreements in the cloud-IoT, smart grids, pervasive edge computing, CPS, 5G networks, WSN, ad hoc networks, e-health clouds, SIP, and multi-server architectures. He received the Top Peer-Reviewer Award from Publons, in 2018, with 126 verified reviews. He is serving as an Academic Editor for SCN and MPE journals (Hindawi). Moreover, he is serving as a Guest Editor for SCN, JHE (Hindawi), and CMC (Techscience)-based special issues. He served as a reviewer for more than 40 reputed journals, including IEEE SYSTEMS JOURNAL, *IEEE Communications Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *IEEE Consumer Electronics Magazine*, IEEE SENSORS JOURNAL, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE INDUSTRY APPLICATIONS SOCIETY, *Computer Networks*, *Information Sciences*, *CAEE*, *Cluster Computing*, *AIHC*, *JNCA*, and *FGCS*.