Secure and Reliable Authentication Protocol for Energy Internet-Enabled Vehicle-to-Grid Communication System

Akber Ali Khan, Samar Muti, *Member, IEEE*, Bander A. Alzahrani, Ashok Kumar Das, *Senior Member, IEEE*, Matloub Hussain, Azeem Irshad, and Shehzad Ashraf Chaudhry, *Senior Member, IEEE*

***Abstract*— As an innovative approach to distributing renewable energy, the Energy Internet (EI) utilizes computing and communication technologies to transform traditional electric power and intelligent transportation systems into an environment that supports open innovation. EI enables bidirectional, sustainable energy transmission between electric vehicles and service providers, facilitating seamless energy exchange. However, the underlying public data communication architecture in Vehicle-to-Grid (V2G) environments is susceptible to several security attacks, which call for an efficient authentication protocol to provide a secure communication channel between the V2G entities. In this article, we introduce a secure and resource-efficient authentication protocol for the reliable distribution of renewable energy in Vehicle-to-Grid systems. The informal and formal analyses presented in this article demonstrate that the proposed scheme is resilient against several known threats. Moreover, the security of the proposed system is verified using the automated simulation tool AVISPA. The proposed scheme completes an authentication round in just 31.337 ms by exchanging 896 bits and two messages. The proposed protocol reduced computational 55%, communication by 73%, while energy consumption reduced to 55% of the mean value of existing protocols. This reduction of costs, along with its attack resistance and comparable security features, shows that the proposed protocol is reliable and robust for secure V2G communication. Thus, the proposed protocol can be applied in a real-time EI-enabled V2G environment.**

***Index Terms*— Vehicle-to-Grid (V2G), authentication, energy internet, security and privacy, key agreement, AVISPA, random oracle model.**

Received 25 September 2025; revised 19 November 2025; accepted 10 December 2025. Date of publication 15 December 2025; date of current version 25 March 2026. This work was supported by the Deanship of Scientific and Research (DSR) at King Abdulaziz University, Jeddah, under Grant RG-3-611-41. The work of Samar Muti and Shehzad Ashraf Chaudhry was supported by Abu Dhabi University's Office of Research and Sponsored Programs under Grant 19300962. *(Corresponding author: Shehzad Ashraf Chaudhry.)*

Akber Ali Khan is with the Department of Applied Sciences and Humanities, IIMT College of Engineering, Greater Noida, Uttar Pradesh 201310, India (e-mail: cs.akberkhan@gmail.com).

Samar Muti is with the Department of Information Technology, College of Engineering and Computing, Liwa University, Abu Dhabi, United Arab Emirates (e-mail: samar.muti@lu.ac.ae).

Bander A. Alzahrani is with the Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: baalzahrani@kau.edu.sa).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seongbuk-gu, Seoul 02841, South Korea (e-mail: ashok.das@iiit.ac.in).

Matloub Hussain is with the College of Business Administration (COBA), University of Sharjah, Sharjah, United Arab Emirates (e-mail: Matloub.Hussain@sharjah.ac.ae).

Azeem Irshad is with the Faculty of Computer Science, GGC Asghar Mall Rawalpindi, Punjab Higher Education Department, Pakistan, and also with the Jadara Research Center, Jadara University, Jordan (e-mail: irshadazeem2@gmail.com).

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Istanbul Nişantaşı University, 34398 Istanbul, Türkiye (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/TCE.2025.3644135

I. Introduction

ELECTRIC vehicles (EVs) have gained increased attention from governments, businesses, and consumers due to growing concerns about clean energy and environmental challenges. EVs are widely considered to be among the best ways to decrease reliance on oil and gas emissions while improving energy conversion efficiency [1]. In the past ten years, the global community has enthusiastically adopted sustainable green energy sources. At the same time, carbon taxes have been more rigorously enforced to address the challenge of global climate change [2]. During the past decade, the global shift towards cleaner and greener energy sources has necessitated the widespread adoption of electric vehicles as a primary mode of transportation. The production of electricity from renewable sources is growing steadily. More and more people are choosing renewable energy options because they emit less carbon and provide cleaner energy compared to conventional methods that are harmful to the environment. A new technology has emerged that allows excess power generated from renewable energy sources to be fed back into the existing grid. This surplus energy, produced by renewable sources in both industries and households, can be contributed to the grid, helping to generate and distribute electricity. In return, the electric boards compensate these contributors for their input. This technology is also expanding to battery operated and electric vehicles, which can now supply excess energy to the grid, a process known as Vehicle-to-Grid technology [3]. Electric vehicles can take in extra power produced by renewable energy sources through different charging methods. They can also supply power back to the grid during times of low power generation, stabilizing grid operations through vehicle to grid [4]. The introduction of V2G technology and the integration of renewable energy sources

like wind and solar power into the grid are opening the door to a more efficient and sustainable energy system. In India, for example, around 70 percent of electricity is generated from conventional sources, with the remaining 30 percent coming from non conventional sources, including renewable energy. The increasing adoption of renewable energy for household and industrial purposes is contributing to lower carbon emissions and cleaner energy. In the transportation sector, electric vehicles are emerging as a promising solution, gaining significant traction in the vehicle market. Economic studies predict that in the future, internal combustion engine vehicles will be replaced by EVs. According to the Australian Energy Market Commission, by the year 2020, the share of new vehicle sales accounted for by EVs is projected to be less than 10 percent. However, after 2020, this share is expected to increase further, accounting for 15 percent to 40 percent of new light vehicle sales [5]. EVs can supply excess energy to the grid, enhancing electricity generation and distribution, and offering substantial benefits for a sustainable future. This transition is significantly supported by Vehicle-to-Grid technology, which enables electric vehicles to not only draw power from the grid, but also return excess electricity back to it. This two way energy flow improves smart grid sustainability, balances load fluctuations, and optimizes power demand [6]. However, realizing the full potential of V2G requires overcoming several challenges, including developing robust business models, and advancing technological solutions. With collaboration and innovation, V2G could play a crucial role in the future of clean energy and transportation. V2G networks enable bidirectional power flow between EVs and the grid, creating a dynamic ecosystem that offers numerous benefits, including grid stability, renewable energy integration, and economic incentives. As the world moves towards a cleaner and more sustainable energy future, the integration of electric vehicles into the power grid has become a significant area of research and development. Vehicle-to-Grid networks have emerged as a trans formative solution that leverages the capabilities of EVs to not only consume energy from the grid but also contribute back to it. Two-way power flow between EVs and the electric grid is made possible by V2G networks, which provide a dynamic ecosystem with several advantages like as grid stability, integration of renewable energy, and financial incentives [7]. However, realizing the full potential of V2G requires overcoming several challenges, including developing robust business models, security and privacy and advancing technological solutions. With collaboration and innovation, V2G could play a crucial role in the future of clean energy and transportation.

A. Motivation and Contribution

The vehicle to grid communication systems have serious concerns about protecting the security and privacy of data relating to vehicle users. In V2G communication systems, personal information is regularly transmitted by communication technologies. This enables attackers to intercept the communication channel and acquire sensitive information about vehicular users. This makes it possible for attackers to eavesdrop on conversations and obtain private data of electric vehicular users. In order to protect network connections in the V2G environment a number of authentication protocols have been proposed each has pros and cons of its own. These include identity based, public key based, and lightweight protocols. Public key based protocols require key pairs for authentication. Identity based authentication relies on identifiable user information for verification, which can pose a security risk if such information is exposed or compromised. The purpose of lightweight protocols is to reduce computational and communication overhead on devices with limited resources. However, their simplified architecture can make them more vulnerable to certain types of attacks. This motivates the development of a security protocol for V2G that protects V2G applications from cyberattacks while ensuring that sensitive information remains accessible only to authenticated users. To address the challenges previously identified in V2G networks, we explore certificateless cryptography as a promising solution for enabling secure communication between vehicles and servers. The proposed protocol aims to ensure the confidentiality, integrity, and availability of user data. The key contributions of this work are summarized as follows:

- This paper design a mutual authentication and key agreement protocol for V2G communication systems for secure communication.
- The proposed protocol preserves a number of cryptographic characteristics and is secure against various active and passive attacks.
- This paper evaluate the security of the proposed protocol through informal analysis and formal analysis including probabilistic RoR model.
- Also, evaluated the formal security analysis by using AVISPA security tool which shows that the proposed protocol satisfies the necessary security requirements.
- Security and performance of proposed protocol have been calculated and compared with other existing related authentication protocols.

B. Composition of the Article

The remainder of the article is organized as follows: Section II outlines the preliminary steps. In Section III, we discuss the related work for V2G communication system. Section IV provides a proposed protocol detailed explanation. Section V provides security evaluation. Section VI includes a performance evaluation analysis. We discuss the limitation and assumptions in section VIII. Finally, the concluding section summarizes the findings.

II. Preliminaries

This section introduces notation used in this paper, system model, threat model, and Biometric and fuzzy extractor essential for understanding and formulating the proposed protocol.

A. System Model

This section describes the system model for V2G network communication, as shown in Figure 1. The model includes a

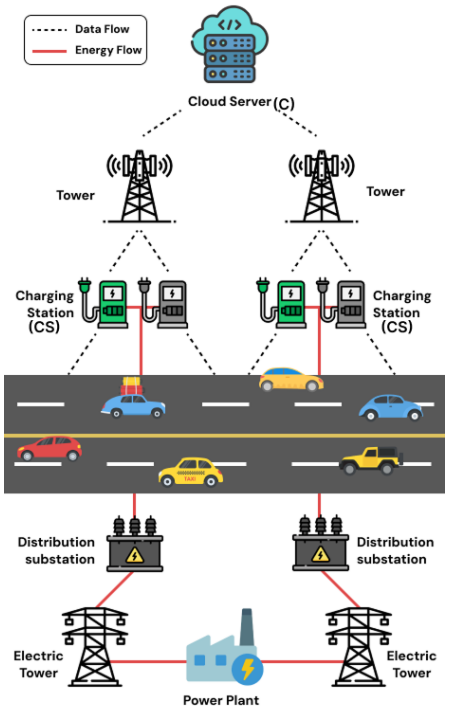

Fig. 1. System Model.

utility service provider, an electric vehicle, and a cloud server. The proposed model enables hierarchical communication, such as between the electric vehicle and the charging station, charging station to cloud server, as well as between the charging station and the utility service provider. The proposed model incorporates an anonymous, lightweight, and robust protocol designed to facilitate secure and efficient communication in V2G networks. A privacy preserving, key exchange and authentication Protocol is incorporated into the proposed system model to enable secure and efficient communication in V2G networks. In V2G environments, there is a critical need for charging stations equipped with parallel processing capabilities to manage communications and energy transactions from multiple vehicles simultaneously. In the proposed system model, the cloud server monitors and controls both the charging station and the electric vehicle users in real time. When a vehicle exits the smart city boundary, the cloud server instructs the charging station to initiate a connection with an alternative cloud server. Hence, the proposed system model offers a promising solution for achieving privacy preserving, secure, and efficient communication within V2G Communication Systems.

B. Security Requirements

Let us make an assumption about the adversary capabilities based on the application before examining security needs. The proposed protocol primary goal is to offer conditional privacy for authentication. The following security objectives must be met in order to achieve these features.

- *Confidentiality:* Energy transaction data is extremely private, and no unauthorized party should be able to access its exact content. For this reason, the communication content must be kept secret throughout the whole V2G key agreement and authentication process, either between the server and the aggregator or between the EV and the server. Attackers may intercept various messages, but they are unable to access or understand their content.
- *Control over unsecured channel:* Any communication sent over the open channel can be intercepted, altered, deleted, and resent by $\mathcal{A}$, who has complete command over the open, unprotected channel. $\mathcal{A}$ may be able to monitor and alter the data stream using this capacity, which could result in data corruption, information leakage, or the delivery of inaccurate information.
- *Tracking ability:* $\mathcal{A}$, might monitor the aggregators and track the location or activity of EVs. This poses a significant threat to personal privacy and could enable $\mathcal{A}$ to execute more precise attacks, such as targeting specific users or devices.
- *Password space traversal ability:* If $\mathcal{A}$ has any other secret knowledge, it can explore the password space in polynomial time. This capability allows $\mathcal{A}$ to perform a brute force attack to guess the password. Consequently, $\mathcal{A}$ can effectively compromise password-protected systems, gaining access to sensitive data or carrying out unauthorized operations.
- *Session key consistency:* The goal of key agreement is to ensure that the parties involved in communication system can securely establish a shared key for all subsequent sessions. To achieve this, the key agreement process must guarantee that the keys computed by all parties are identical.
- *Resistance against known attacks:* The protocol must be secure against impersonation attack, replay attack, main-in-the-middle attack, and modification attack.
- *Unlinkability:* This property ensures that an attacker cannot relate the captured messages to any of the past as well as future messages from the same communicating entities
- *Malicious vehicle traceability:* $\mathcal{A}$ can determine the true identification of the vehicle users in the event of malicious activity. But no vehicle is capable of doing this.
- *Privacy:* When a vehicle receives information, it can determine the true identify of the source vehicle user.
- *User anonymity:* Attacks like message interception and eavesdropping must prevent unauthorized parties from gaining access to an EV owner's personal data. In other words, even if an adversary obtains messages from the V2G system, they should be unable to identify the EV associated with the messages or correlate different pieces of information to track the EVs location or activities.
- *Authentication:* The V2G system must enable mutual authentication between the grid server and the electric vehicle user prior to starting energy transactions. In order to simplify critical agreement between the grid server and electric vehicle users and ensure reliable and secure energy transactions, the grid server ultimately serves as an intermediary authentication entity.

TABLE I
NOTATIONS AND ASSOCIATED DESCRIPTION

Notation	Explanation
$\mathcal{A}$	Adversary
ΔT	Maximum transmission delay
ID_i	The unique identity of entity i
C	Cloud server
$h(.)$	Secure one way hash function
PW_i	Password of V_i
K_i	Secrete key of entity i
K_C	Secrete key of C
g	Generator of ECC
$.$	Scalar multiplication operation on ECC
V_i	Vehicular user i^{th} entity
$\stackrel{?}{=}$	Whether equal or not
p, q	Sufficiently large prime
$\oplus$	The bitwise XOR operation
B_i	Biometric of V_i
$\|\|$	Concatenation operation
SK_i	The session key of entities i
$\cong$	Approximate number

C. Threat Model

We adopt the Canetti-Krawczyk (CK) adversary model as the foundational framework [8]. Recognized as a benchmark in key exchange protocol analysis, the CK model provides a more comprehensive and realistic threat perspective than the Dolev Yao (DY) model [9]. Under this model, it is essential for key exchange protocols to ensure the resilience of the established session key against both temporary (short-term) and permanent (long-term) secret leakage. This requirement underscores the need for robust authentication protocol that maintain session key security even in the presence of partial key exposure. The proposed protocol operates through several communication stages. In the first stage, the user registers with the cloud server using a secure communication channel. After registration, the execution phase begins, where electric vehicles user and cloud server exchange data over an unsecured public channel. This process follows the DY threat model [9] as discussed above which assumes that attacker may intercept, alter, or remove messages during communication.

D. Notations

The related useful notations are displayed in Table I.

E. Biometric And Fuzzy Extractor

The user biometric impression is used by a cryptographic technique known as the fuzzy extractor [10] to eliminate potential noise. A fuzzy extractor mathematical representation is $(\mathcal{L}, \mathcal{J}, \mathcal{M})$, where $\mathcal{M}$ is the biometric input of data of metric space of finite dimension and $\mathcal{L}$ is the bit length of the output string. The $Gen(.)$ function and the $Rep(.)$ function are the two algorithms that the fuzzy extractor uses.

- $Gen(.)$: The $Gen(.)$ is a probabilistic approach that incorporates biometric $B_i \in \mathcal{M}$ input and gives secret key data $\Re_i \in \{0, 1\}^l$ as output and τ_i a public reproduction variable for the bio-metric input data $B_i \in \mathcal{M}$. Where $Gen(B_i) = \{\Re_i, \tau_i\}$.
- $Rep(.)$: A biometric data is used in a deterministic method $B_i' \in \mathcal{M}, \mathcal{T}$ and the attribute τ_i then replicate bio-metric key $\Re$ that is $Rep(\tau_i, B_i') = \Re_i$, provided $d(B_i, B_i') \leq \mathcal{J}$.

III. RELATED WORK

In order to allow electric vehicles to function as both energy consumers and energy storage devices that can provide power to the grid, two-way communication is made possible using a technology known as V2G. Nonetheless, both domestic and international researchers have focused a great deal of emphasis on V2G security and privacy issues. Wu and Zhou [11] presented a protocol that combines elliptic curve public key encryption with symmetric key approaches. Benefits of this protocol include efficiency and excellent scalability. Even so, Xia and Wang [12] pointed out that the protocol given in [11] is vulnerable to man-in-the-middle attacks and suggested a key distribution and authentication framework based on a reliable third party, which has been proven to be effective against these types of attacks. The batch authentication protocol for V2G networks was presented by Guo et al. [13]. However, this protocol is merely a variant of the conventional DSA algorithm and does not offer security against other network threats or privacy protection for critical vehicle data. To ensure unlinkability between issued permits and the real identities of electric vehicles, Yang et al. [14] design a privacy-preserving protocol employing identity based restrictive partially blind signature technology. As noted by Park et al. [15], the protocol described in [12] is entirely dependent on the security of the underlying cryptographic technic and cannot be protected against impersonation and unknown key sharing attacks. Chen et al. [16] design key agreement and authentication scheme which permitted charging and discharging stations to perform anonymous mutual authentication and dynamic management of EV. But even so, there is a substantial overhead associated with the technique during the vehicle revocation procedure. However, Wang et al. [17] identified that the scheme given by Yang et al. [14] lacks a formal security specification for the V2G network system, rendering it vulnerable to realistic adversarial models. To mitigate these shortcomings, Wang et al. [17] design a key agreement protocol, whose security properties were rigorously proven under a formal security analysis. Saxena and Choi [18] proposed a two factor key agreement authentication design leveraging bilinear pairing to enhance authentication efficiency while ensuring forward privacy, message integrity and identity anonymity. However, the protocol does not support traceability mechanisms to identify and track malicious vehicles. Tsai and Lo [19] proposed a key exchange protocol utilizing identity-based encryption and signature schemes to achieve mutual authentication and confidentiality. After that, Odelu et al. [20] highlighted that the framework of Tsai and Lo [19] does not provided the privacy and security of long-term private parameters of smart meters. Therefore, Odelu et al. [20] design protocol to mitigate the highlighted attacks. Additionally, Abdallah and Shen [21]

developed a key establishment approach for the V2G architecture. They simply provide the informal security analysis of their protocol. Shen et al. [22] proposed an authentication protocol tailored for V2G networks, incorporating a self-synchronization method to preserve privacy and secure session keys. However, the protocol fails to provide location privacy for electric vehicles. While it reduces computational overhead, the scheme incurs substantial storage overhead due to the aggregation of vehicle user authentication data. A bilinear paring-based protocol with three-factor authentication was also developed by Li et al. [23] for a smart V2G network in global mobile networks. Gope and Sikdar [24] introduced a energy internet framework for V2G communication, enabling charging and discharging across geographically distributed stations. However, the pseudonym scheme employed does not guarantee full anonymity, and the risk of collusion between semi-trusted service providers and external adversaries poses significant privacy threats to users. Garg et al. [25] proposed a blockchain-based key exchange and authentication framework for V2G systems, accompanied by a formal security analysis to validate its robustness. Roman et al. [26] presented a V2G network protocol. In order to create safe key generation and secret exchange procedures, their protocol successfully combines bi-linear mapping and Elliptic Curve Diffie-Hellman hard problem. Bansal et al. [27] presented a key agreement and authentication framework that uses physically unclonable functions, EV anonymity is not guaranteed by the protocol. Irshad et al. [28] subsequently conducted a security analysis on [24] and showed that replay and MITM attacks are vulnerable with their scheme. They added that their scheme had desynchronization problems, which could cause a major problem in which the ESP is still unable to identify the real user. In order to address the shortcomings in Gope and Sikdar protocol [24], Irshad et al. [28] recently developed an enhanced protocol to increase security against known threats. However, we thoroughly examined the Irshad et al. [28] scheme and found that any attacker with public channel parameters and a verifier could readily impersonate the user. Further, because the ESP doesn't identify the user prior to use, it is inaccurate during the verification process. Also, absolute forward and backward secrecy is not provided by their protocol. Su et al. [29] introduced a privacy-preserving authentication technique for V2G communication networks. This protocol uses Elliptic Curve Cryptography to offer authentication automobiles cars and electric vehicle central stations. However, the framework given by Su et al. [29] was shown to have weaknesses by Sureshkumar et al. [30]. Ahmed et al. [31] design a protocol based on the energy internet that uses signcryption and unsigncryption techniques in a V2G communication. However, this protocol fails to guarantee the forward security of session keys and fails to ensure the privacy of vehicle data. Rajasekaran et al. [32] designed a key agreement framework that might be used in a number of V2G use cases, including smart grid management, energy trading, and EV charging. But because of the energy-intensive tasks it completes, its energy efficiency is degraded, and its scalability is limited. Ascon is a symmetric encryption technique that employe by Hou et al. [33] to ensure secure communication between the electric vehicles and the charging station throughout the charging reservation procedure. Shamshad et al. [34] designed an access control protocol for EI-based V2G network. Unquestionably, a variety of authentication techniques have been design for the EI-based V2G network to preserve and secure sensitive data. However, the evidence indicates that the majority of the protocols covered above are either computationally unfeasible for an EI-based V2G framework with limited resources or ignore important security features like impersonation and anonymity. These facts have inspired us to design a secure and effective mutual authentication key agreement protocol for the EI based V2G communication environment in order to address the shortcomings that have been found. The security aspects of the developed protocol are superior to those of their related protocols.

IV. The Proposed V2G Protocol

In this section, we describe our proposed protocol. The protocol utilizes, ECC, collision resistant hash function, and bit-wise XOR operation to accomplish mutual authentication. The vehicle user and the charging station first registers with C then communicate with key agreement process each other.

A. Initialization Phase

In the initialization phase, the proposed protocol executes several key tasks. Initially, cloud server computes p, $E_q(a,b)$: $\beta^2 = \alpha^3 + a\alpha + b \ mod \ q$ where $a, b \in Z_q^*$ and $4a^3 + 27b^2 \ mod \ q \neq 0$, is known as non singular elliptic curve. The $Gen(.)$ and $Rep(.)$ functions are used to perform biometrics using the fuzzy extractor during the sign-in process. Now the cloud server needs to select $h(.)$ and generates private key $K_i \in Z_p^*$. Finally, the cloud server reveal $\{E_q(a,b), q, g, h(.)\}$, and keeps K_i privately.

B. Registration Phase of Electric Vehicle User

In vehicle user registration phase, user V equipped with SC registers itself with C. The details of registration phase is discussed below:

Step 1. The vehicle user V_i inputs unique identity ID_i, password pw_i, imprints biometric B_i and then computes biometric signature $(\sigma_i, \tau_i) = Gen(B_i)$. Further, user V_i computes $VPWD_i = h(pwd_i \| \sigma_i)$ and sends registration message $M_1 = \{ID_i, VPWD_i\}$ to C on a secure channel.

Step 2. On receiving registration message M_1, C, verify V_i after that generates NID_i as a pseudo identity, and computes $CSP_i = h(K_c \oplus ID_c)$. Further, C Computes following hashed values $CR_1 = CSP_i \oplus h(VPWD_i \| ID_i)$, $CR_2 = h(ID_i \| VPWD_i \| CSP_i \| NID_i)$, $AV_1 = NID_i \oplus h(ID_i \oplus VPWD_i)$, and $AV_2 = ID_i \oplus h(K_c \| ID_c)$. Furthermore, C includes $\{AV_2, CID_i\}$ in database corresponding ID_i and sends response $M_2 = \{AV_1, CR_1, CR_2\}$ to vehicle user V_i.

Step 3. On receiving response message M_2, vehicle user V_i computes $CID_i = AV_1 \oplus h(ID_i \| VPW_i)$ and $CR_3 = CID_i \oplus h(HPW_i \| ID_i)$ and stores the data $\{CR_1, CR_2, CR_3, \tau_i\}$ in smart device.

TABLE II
SUMMARY OF LIMITATIONS/DRAWBACKS OF RELATED SCHEMES

Scheme	Year	Cryptographic Method used	Properties
Bansal et al. [27]	2020	Physical unclonable function and HMAC	Provides low computation cost and energy efficiency, Vulnerable to privilege insider and physical attacks and lacks user anonymity and untraceability.
Irshad et al. [28]	2021	One way hash function	Protocols does not secure against impersonation attacks and stolen verifier attacks.
Ahmed et al. [31]	2021	Hash function	Threatened by the adversary
Rajasekaran et al. [32]	2022	ECC	The energy efficiency of the protocol compromised and system scalability is limited.
Sureshkumar et al. [35]	2022	One way hash function	Provide high level security features with low computing costs. Session key leak attacks are possible, impersonation attacks are not secure, and mutual authentication is not provided.
Hou et al. [33]	2023	Ascon	Does not maintain compatibility with earlier network versions.
Reddy et al. [36]	2023	Physical unclonable function	Present lightweight authentication for V2G Environment, does not secure against password guessing attacks.
Yu et al. [37]	2024	Physical unclonable function	Protocol does not secure against ephemeral secret leakage attacks and vulnerable to tracing attacks.
Ahmed et al. [38]	2024	Physical unclonable function	Protocol does not secure against known session specific temporary information and ephemeral secret leakage attack.
Yu and Park [37]	2024	Physical unclonable function	Does not provided mutual authentication, session key security and stolen verifier attack resilience
Xu et al. [39]	2025	Symmetric encryption and hash functions	Present a key agreement scheme for vehicles to infrastructure network, not secure against resists impersonation attack, DoS attack resilience and stolen verifier.

C. Registration Phase of Charging Station

The details of service provider registration phase is discussed below.

Step 1. Firstly, CS input the identity as ID_{CS} and then sends its own $\{ID_{CS}\}$ to cloud server through a secure channel.

Step 2. Cloud server verify existence of CS in its database, then C retrieve the values $\{CID_i, AV_2\}$ in database. Further, Cloud server computes $ID_i = AV_2 \oplus h(K_c \| ID_c)$, $ID_i = AV_2 \oplus h(K_c \| ID_c)$, $SP_1 = CSP_i \oplus h(ID_i \| ID_{cs})$ and $SP_2 = ID_{cs} \oplus h(ID_c \| K_c)$ and store $\{SP_2\}$ in its database for futher communication. After that C sends $\{ID_i, CID_i, SP_2\}$ to CS via secure channel.

Step 3. Receiving the message $\{ID_i, CID_i, SP_2\}$ from C, CS computes the followings parameters $CSP_i = SP_1 \oplus h(ID_i \| ID_{cs})$ and $CSP_{cs} = CSP_i \oplus h(ID_{cs} \| K_{cs})$ and then store $\{CSP_{cs}\}$ in database for future communication. Further, CS computes $PID_i = ID_i \oplus h(CID_i \| K_{cs})$ and also store $\{CID_i, PID_i\}$ in database.

D. EI-Based V2G Authentication Environment

The detailed description of the login, authentication and key agreement phase is given below:

Step 1. Vehicle user V_i inputs the parameters ID_i', pw_i' and B_i' and computes the followings values as $\sigma_i' = Rep(B_i', \tau_i')$, $VPW_i' = h(pw_i' \| \sigma_i')$, $CSP_i' = CR_1 \oplus h(VPW_i' \| ID_i')$, $CID_i' = CR_3 \oplus h(ID_i' \| \tau_V' \| pw_i' \| VPW_i')$ and $CR_2' = h(ID_i' \| VPW_i' \| CSP_i' \| CID_i')$. After that vehicle user V_i verifies $CR_2' \stackrel{?}{=} CR_2$ if yes, then generates random value $a \in Z_q^*$ and time stemp t_1. Further, Computes $V_i = a.g$, $\alpha_1 = h(ID_i' \| V_i \| t_1)$, $\beta_1 = V_i \oplus h(CID_i \| ID_i' \| t_1)$ and $\gamma_1 = CID_i \oplus h(CSP_i' \| t_1)$. Further, sends message $M_1' = \{\alpha_1, \beta_1, \gamma_1, t_1\}$ to charging station.

Step 2. On receiving M_1', the service provider SP verifies $t_2 - t_1 \leq \triangle t$ and computes the following parameters $CSP_i' = CSP_{cs} \oplus h(K_{cs} \oplus ID_{cs})$ and $CID_i = \gamma_1 \oplus (h(CSP_i' \| t_1)$. After that SP, verifies PID_i against CID_i in database if yes then computes $ID_i' = PID_i \oplus h(CID_i \| K_{cs}$, $V_i' = \beta_1 \oplus h(CID_i \| ID_i' \| t_1)$ and $\alpha_1' = h(ID_i' \| V_i' \| t_1)$. Further, verifies $\alpha_1' \stackrel{?}{=} \alpha_1$ if yes then generates a random number as $b \in Z_q^*$ and computes $X = b.V_i'$, session key agreement as $SK_{sp} = h(ID_i' \| ID_{cs} \| X \| (t_1 \oplus t_2))$. Furthermore, service provider SP, computes $J = b.g$, $Q = J \oplus h(ID_i' \| V_i' \| t_2)$, $F = ID_{cs} \oplus h(ID_i' \| J \| X \| t_2)$ and $Z = h(ID_{cs} \| J \| SK_{sp} \| t_2)$. Sends the message $M_2' = \{Q, F, Z, t_2\}$ to vehicle user V_i.

Step 3. On receiving $M_2' = \{Q, F, Z, t_2\}$, V_i verifies $T_3 - T_2 \leq \triangle t$ and computes $J' = Q \oplus h(ID_i' \| V_i \| t_2)$, $X' = J'.a$, $ID_i' = F \oplus h(ID_i' \| J' \| X' \| t_2)$, session key agreement as $SK_{vu} = h(ID_i' \| ID_{cs}' \| X' \| (t_1 \oplus t_2))$. Also verifies $Z = h(ID_{cs}' \| J' \| SK_{sp} \| t_2)$ for secure communication.

V. SECURITY ANALYSIS

In this section, we investigate the security of our proposed protocol against various network attacks. To check security, we have provided formal and informal security assessments. To formally evaluate the security of the private parameters used in our proposed protocol, we have used a tool called AVISPA to implement our protocol. This security tool evaluates network security protocols against all types of active and passive attacks in the network. In addition, in the informal analysis, to ensure the security of the proposed protocol. Further, we conducted a comprehensive assessment of potential network vulnerabilities and demonstrated its resistance to these vulnerabilities through the utilization of specific techniques.

A. Informal Security Analysis

This subsection demonstration of how the proposed protocol is protected against all well known security threats. Also, we explains how the designed protocol satisfies the necessary security requirements. The necessary security attacks and properties of the V2G system are broken down as follows:

1) Replay Attack: The malevolent opponent attempts to intercept and resend a previously transmitted message in order to launch a counterattack. However, the protocol incorporates verifying conditions, random nonces, and a secure hash function within the messages. These elements ensure that each message is unique and can be validated for authenticity and freshness, thereby preventing the reuse of old messages. Hence, the proposed protocol is resistant to replay attacks.

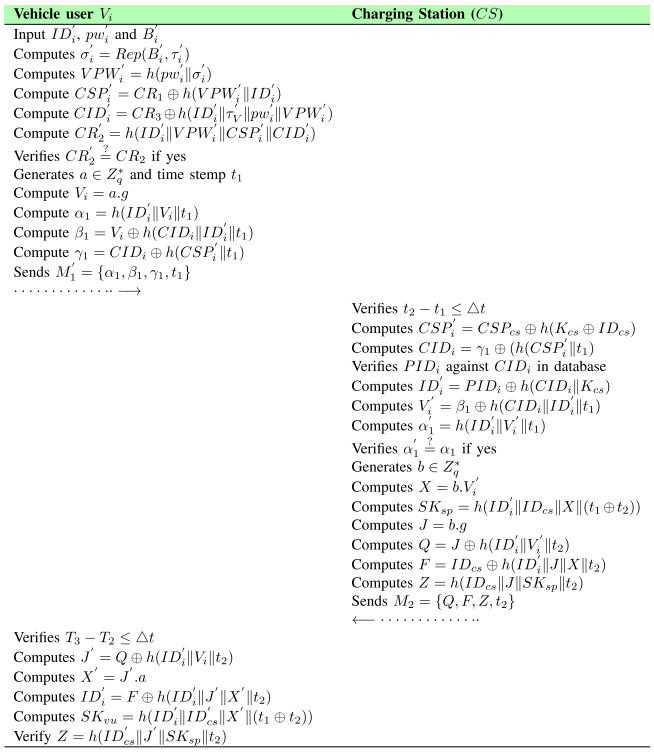

Fig. 2. EI-based V2G authentication phase.

2) Key Freshness: Key freshness refers to the generation of new cryptographic keys to ensure that future communications remain secure, even if older keys are compromised. To maintain freshness, it is common practice to incorporate a random nonce and a timestamp when establishing new keys. In the proposed protocol, a fresh random integer and timestamp are generated at every step. This approach effectively guarantees that the keys remain fresh and resilient against replay or compromise, thereby enhancing the overall security of the system.

3) Anonymity Property: For the messages transmitted in the public channel of the proposed protocol, they do not contain the identity of any legal entities, whether in the form of plaintext or ciphertext. In this way, it is computational infeasible for attackers to obtain an identity of certain legitimate participant, and the proposed protocol can support anonymity for this reason.

4) Mutual Authentication: The vehicular user computes $\alpha_1 = h(ID_i' \| V_i \| t_1)$ and sends this with $M_1 = \{\alpha_1, \beta_1, \gamma_1, t_1\}$ to service provider the authentication process in the service provider side is realized by verifying whether Verifies $\alpha_1' \stackrel{?}{=} \alpha_1$ where $\alpha_1' = h(ID_i' \| V_i' \| t_1)$. After that, CS sends $M_2 = \{Q, F, Z, t_2\}$ to vehicular user, the authentication process in the user side is accomplished by checking the equation $Z = h(ID_{cs}' \| J' \| SK_{sp} \| t_2)$. Thus, the property of mutual authentication is supported in the proposed protocol.

5) Eavesdropping Attack: According to this attack, the adversary can intercept all messages transmitted over the public channel. However, in the proposed protocol, all parameters are protected using a biometric fuzzy extractor function combined with fresh random numbers generated in each round of authentication. This ensures that the adversary cannot successfully guess or reproduce any sensitive parameters. Therefore, the proposed protocol is secure against eavesdropping attacks.

6) Impersonation Attack: The proposed scheme can support the security under impersonation at tack in both two situations of user impersonation attack and service provider impersonation attack. If the attacker tries to impersonate as a legitimate user by intercepting and modifying the transmitted messages $M_1 = \{\alpha_1, \beta_1, \gamma_1, t_1\}$, then the action will be detected and the related session will be refused due to the authentication verification of the service providers $\alpha_1' \stackrel{?}{=} \alpha_1$. In addition, if the at tacker attempts to impersonate as a valid service provider by intercepting and modifying transmitted messages $M_2 = \{Q, F, Z, t_2\}$, then it will fail due to the user's authentication verification $Z' \stackrel{?}{=} Z$.

7) Man-in-The-Middle Attack: There are two messages $\{\alpha_1, \beta_1, \gamma_1, t_1\}$ and $\{Q, F, Z, t_2\}$ which are exchanged between V_i and CS to complete authentication and key agreement process. To mount man-in-the-middle attack, adversary tries to manipulate these messages to create another valid message. But in proposed protocol, both of these messages are protected by shared secret and collision resistant hash function. So, to do valid modifications to messages, MIM attacker needs to steal secret and find collision in $h(.)$ in polynomial time which is computationally infeasible.

8) Smart Device Stolen Attack: Assume that an attacker has taken the user smart device and the important data $\{CR_1, CR_2, CR_3, \tau_i\}$ retrieved by the attacker from the smart device. Consequently, the attacker cannot computationally derive the identification information NID_i and ID_i because they are unfamiliar with the V_i password and biometric. Further, if the vehicle user device is lost or stolen, an attacker cannot impersonate the legitimate user without having access to their identity, password, and masked credentials. Moreover, due to the incorporation of random values, it is computationally infeasible for an adversary to guess the password within polynomial time. Therefore, the proposed scheme ensures strong resistance against offline password guessing and stolen device attacks.

9) Stolen Verifier Attack: Suppose the attackers have the capacity to obtain the verifier table CID_i, PID_i from charging station, where $PID_i = ID_i \oplus h(CID_i \| K_{cs})$ then they are unable to disclose the pertinent ID_i without the service provider's long-term key K_{cs} knowledge. The proposed protocol is resistant to stolen verifier attacks.

10) Known Key Secrecy: Session key security prevents adversary from successfully computing current session key irrespective of having access to old session keys. In proposed protocol SK for current session is computed as $SK = h(ID_i' \| ID_{cs}' \| X' \| (t_1 \oplus t_2))$ in which a and b are two session specific random nonce which makes this key unique to each session.

11) Privilege Insider Attack: Assume that the attacker is a legitimate insider user $\mathcal{A}$ and attempts to obtains some critical information about other users or service provider, then it is computational infeasible for $\mathcal{A}$ to extract C secret key K_c, identity ID_c or other user critical parameters. Because in the registration information $\{AV_1, CR_1, CR_2\}$ sent back from C

to $\mathcal{A}$ one way hash function is utilized to protect cloud server long-term secrets and involved information does not have any of uniform parts as other users. It is computational infeasible for the attacker to extract legitimate users identities without the knowledge of C secret key K_c and identity ID_c. Therefore, the proposed scheme can provide the security under privilege insider attack.

12) Offline Password Guessing Attacks: Assuming that the adversary can obtain the parameters stored in the vehicle through side channel attacks, namely CR_1, CR_2, CR_3, but since the adversary cannot obtain the corresponding response CR_i, they cannot verify $CR_2' \stackrel{?}{=} CR_2$ to guess the users identity and password. Only by initiating online guessing attacks can the adversary determine the correct password, and hence our proposed protocol can resist offline password guessing attacks.

13) DoS Attack: In this attack, an adversary might attempt to paralyze a certain entity (V_i, CS) by repeatedly replaying old messages. However, for example, CS initially checks if the time stamp meets the condition $t_2 - t_1 \leq \triangle t$. If this condition fails to hold, CS immediately ends the session. Further, even if adversary changes the timestamp to make the forged timestamp less than the set value, the CS still ignores this message since the verification failure in hash value $\alpha_1' = h(ID_i' \| V_i' \| t_1)$, which is calculated by original timestamp. Thus, such denial-of-service attack is rendered invalid.

14) Secret Leakage Attack: In this attack, the CK adversary can compute the session key through obtaining temporary secrets like random values a and b. Factually, in the proposed protocol, in addition to random values a and b it contains long-term secret $a.g$ and $b.g$ that also participates in the establishment of the session key. Therefore, even if the adversary has access to random values a and b, adversary still cannot verifies $\alpha_1' \stackrel{?}{=} \alpha_1$. Thus, this attack is ineffective.

15) Untraceability: The proposed protocol does not call for any identifying data to be transmitted over a public channel or stored on a vehicle user's device. Instead of ID_i via public channel, we computes $CSP_i' = CR_1 \oplus h(VPW_i' \| ID_i')$ $CID_i' = CR_3 \oplus h(ID_i' \| \tau_V' \| pw_i' \| VPW_i')$ and $CR_2' = h(ID_i' \| VPW_i' \| CSP_i' \| CID_i')$ after that we verifies, $CR_2' \stackrel{?}{=} CR_2$. As a result, only during the communication session can the adversary discover the user CR_2'. Since CR_2' varies depending on the session our suggested protocol is hence untraceable.

B. Formal Security Analysis

This subsection uses the ROR model as the foundation for a formal security analysis of the designed protocol. Each entity is presumed to have multiple instances that take part in various, potentially simultaneous executions of the proposed protocol. Let us define Ω_V^i, Ω_{SP} as user instance of order i and the service provider instance respectively, and any type of instances are denoted by $\Omega \in \Delta$. The adversary $\mathcal{A}$ has the capabilities to interact with Ω_V^i and Ω_{SP} by asking the following queries.

- ***Execute*(Δ):** The purpose of this query is to identify passive eavesdropping attacks and to return all relevant transferred messages in the public channels within Ω_V^i and Ω_{SP}.
- ***Send*($\Omega_V^i, init$):** This query yields the messages sent from Ω_V^i for setting up the authentication procedure.
- ***Send*($\Delta, messages$):** This query is aimed at active attacks by means of modifying and intercepting transcripts, and it responses with corresponding messages dispatched from $\Omega \in \Delta$.
- ***Corrupt*(Ω_V^i, β):** This request is intended to reveal sensitive data that has been inserted into the smart card if $\beta = 1$.
- ***Corrupt*(Ω_{SP}, β):** This query is applied to reveal the long-term private key if $\beta = 1$.
- ***ESReveal*(Δ, β):** This query compromises two ephemeral secrets a and b if $\beta = 1$.
- ***Hash(message)*:** A random number is returned by this query as the hash value of the entered string.
- ***Test*(β):** This request returns a coin C that has been flipped. If C equals 1, the session key SK will be returned by the query. However, if C equals 0, it can only return a random value that has the same length as SK.

Lemma (Difference Lemma): Assume that S represents the error event between S_1 and S_2, the events of the probability density function, in the following way $S_1 \wedge \neg S \iff S_2 \wedge \neg S$, then $|Pr[S_1] - Pr[S_2]| \leq Pr[S]$.

Theorem 1: Suppose that the adversary $\mathcal{A}$ is capable of deploying Send, Execute, Corrupt, Hash, ESReveal, and Test queries in the RoR model. $Adv_{AK}^{\mathcal{A}}$ proposed represents the primary function for adversary A operating within polynomial time to compromise the security of the proposed authentication protocol. further, consider Q_{send}, Q_{hash}, $Adv_{ECC}^{\mathcal{A}}$, L, C', S' denote the number of executing Send queries, Hash queries, the advantage of solving computational ECC problem, the bit length of a transferred message and two constants respectively. It is possible to guarantee the security of the designed authentication scheme, as the value of $Adv_{AK}^{\mathcal{A}}$ is negligible as below:

$$Adv_{AK}^{\mathcal{A}} \leq 2Adv_{ECC}^{\mathcal{A}} + \frac{3Q_{hash}^2}{2^L} + \frac{Q_{end}}{2^{L-2}} + 2C'Q_{send}^{S'} \quad (1)$$

Proof: The game of sequences was introduced to illustrate the semantic security of the designed scheme. The actual attack begins with G_0 and ends with G_6 is the game where $\mathcal{A}$ has no advantage. Let $Pr[\mathcal{E}]$ to be symbolized as the probability of event $\mathcal{E}$, and the probability of a successfully guesses the flip of coin for G_i is denoted by $Pr[Succ_{G_i}^{\mathcal{A}}]$. The queries are simulated on a discursive basis under actual attacks to demonstrate the proposed protocol.

Game G_0**:** Simulating game G_0 is equivalent to conducting a real attack in the random oracle model with no supported queries. The chance of adversary $\mathcal{A}$ successfully breaking the proposed protocol can be expressed as follows.

$$Adv_{AK}^{\mathcal{A}} = |2Pr[Succ_{G_0}^{\mathcal{A}}] - 1|. \quad (2)$$

Game G_1**:** The game G_1 includes Execute query, base upon the foundation of game G_0. In the proposed protocol, adversary $\mathcal{A}$ only acquires messages $\{\alpha_1, \beta_1, \gamma_1, t_1\}$ and $\{Q, F, Z, t_2\}$ through Execute query. Since ID_i, ID_{cs} and X are confidential to $\mathcal{A}$, the session key will not be exposed to $\mathcal{A}$.

$$Pr[Succ_{G_1}^{\mathcal{A}}] = Pr[Succ_{G_0}^{\mathcal{A}}] \tag{3}$$

Game G_2**:** Game G_2, based in game G_1, allows adversary $\mathcal{A}$ to initiate an active attack. In the game G_2, A can only extract the session key $SK = h(ID_i' \| ID_{cs} \| X \| (t_1 \oplus t_2))$= $h(ID_i' \| ID_{cs}' \| X' \| (t_1 \oplus t_2))$ of the proposed protocol by resolving the computational ECC problem and carrying out the Hash query. As per the birthday paradox, the chance of a hash collision is $\frac{Q_{Hash}^2}{2^{L+1}}$ at the most in the Hash query. where L is the hash function length. Therefore, based on difference lemma, we have

$$|Pr[Succ_{G_2}^{\mathcal{A}}] - Pr[Succ_{G_1}^{\mathcal{A}}]| \leq \frac{Q_{Hash}^2}{2^{L+1}} + Adv_{ECC}^{\mathcal{A}} \tag{4}$$

Game G_3**:** Construction on game G_2, game G_3 allows adversary $\mathcal{A}$ to guess the verifiers using the send query. The relationship can be expressed as follows:

$$|Pr[Succ_{G_3}^{\mathcal{A}}] - Pr[Succ_{G_2}^{\mathcal{A}}]| \leq \frac{Q_{Send}}{2^L} \tag{5}$$

Game G_4**:** Based on game G_3, game G_4 offers two methods for adversary $\mathcal{A}$ to break the session key of the proposed protocol. One approach is to break the session key using information from the long-term key, while the other approach involves executing an ephemeral secret leakage attack. $\mathcal{A}$ attempts to execute the $Corrupt(\Omega_{SP}, \beta)$ query in the first scenario. Even if $\beta = 1$ and $\mathcal{A}$ gets Ω_{SP} private key K_{cs}, $\mathcal{A}$ still cannot obtain the session key $SK = h(ID_i' \| ID_{cs} \| X \| (t_1 \oplus t_2))$ due to the fact that $\mathcal{A}$ cannot extract its intrinsic attributes ID_i, X without acquiring PID_i and NID_i. In the second scenario, $\mathcal{A}$ attempts to perform $ESReveal(\Delta, \beta)$ queries. Even if $\beta = 1$ and $\mathcal{A}$ acquires the transient secrets a and b, $\mathcal{A}$ is still unable to obtain the parameters ID_i, ID_{cs}, and X necessary to reconstruct the session key of the proposed protocol. Consequently, for $\mathcal{A}$ in both scenarios, carrying out Send and Hash queries is the possible option available, and the relationship can be formalized as follows:

$$|Pr[Succ_{G_4}^{\mathcal{A}}] - Pr[Succ_{G_3}^{\mathcal{A}}]| \leq \frac{Q_{Send}}{2^L} + \frac{Q_{Hash}^2}{2^{L+1}} \tag{6}$$

Game G_5**:** Developing upon game G_4, game G_5 allows adversary $\mathcal{A}$ to launch a smart card stolen attack and a password guessing attack by using the $Corrupt(\Omega_V^i, \beta)$ query. The chance of $\mathcal{A}$ successfully extracting Ω_V^i password is $C' Q_{send}^{S'}$ Send at most when Q_{Send} times Send queries are permitted for online guessing, and the relationship can be structured as shown below:

$$|Pr[Succ_{G_4}^{\mathcal{A}}] - Pr[Succ_{G_3}^{\mathcal{A}}]| \leq C' Q_{send}^{S'} \tag{7}$$

Game G_6**:** Developing on game G_5, game G_6 offers adversary $\mathcal{A}$ the chance to carry out an impersonation attack. $h(ID_i \| ID_{cs} \| X \| (t_1 \oplus t_2))$, for an adversary $\mathcal{A}$, the only viable option is to directly extract the session key of the proposed protocol. The relationship can be expressed in the following way:

$$|Pr[Succ_{G_6}^{\mathcal{A}}] - Pr[Succ_{G_5}^{\mathcal{A}}]| \leq \frac{Q_{Hash}^2}{2^{L+1}} \tag{8}$$

Based on formulas (2) through (8) derived from the sequences discussed above, the following formula can be established.

$$\begin{aligned} Adv_{AK}^{\mathcal{A}} &= |2Pr[Succ_{G_0}^{\mathcal{A}}] - 1| \\ &= |2(Pr[Succ_{G_6}^{\mathcal{A}} - Pr[Succ_{G_0}^{\mathcal{A}}]) \\ &\quad + 1 - 2Pr[Succ_{G_6}^{\mathcal{A}}| \\ &\leq 2\sum_{n=0}^{5}(|Pr[Succ_{G_{n+1}}^{\mathcal{A}}] - Pr[Succ_{G_n}^{\mathcal{A}}]|) \\ &= 2(\frac{Q_{Hash}^2}{2^{L+1}} + Adv_{ECC}^{\mathcal{A}} + \frac{Q_{Send}}{2^L} + \frac{Q_{Send}}{2^L} \\ &\quad + \frac{Q_{Hash}^2}{2^{L+1}} + C' Q_{send}^{S'} + \frac{Q_{Hash}^2}{2^{L+1}}) \\ Adv_{AK}^{\mathcal{A}} &= 2Adv_{ECC}^{\mathcal{A}} + \frac{3Q_{hash}^2}{2^L} + \frac{Q_{end}}{2^{L-2}} + 2C' Q_{send}^{S'} \end{aligned}$$

C. Formal Security Validation: Simulation Study Using AVISPA Tool

The security strength of the proposed authentication and key agreement scheme for V2G is validated using the AVISPA security tool [40], which makes use of the High-Level Protocol Specification Language (HLPSL) for coding. AVISPA is a comprehensive framework designed to develop and test formal models of security protocols. It is particularly useful for verifying the security of authentication schemes or protocols against a wide range of vulnerabilities.

The AVISPA back-end tool called OFMC & CL-AtSe are used to show and validate cryptographic attacks against the tested authentication scheme. The OFMC and CL-AtSe back-ends were chosen to demonstrate the proposed scheme because bitwise XOR is not supported by SATMC and TA4SP. Mutual authentication, information confidentiality, and the session key are the security goals that AVISPA validates. In the scenario, CL-AtSe and OFMC insert adversary into the conversation with the ability to record and replay the exchanges. If the proposed approach is resilient to cryptographic threats, the result of analysis indicates the SAFE state. If the attack trace is discovered by backends then the result of analysis indicated the UNSAFE state.

The final result of the AVISPA simulation is shown in Figure 3. The AVISPA results indicate that the proposed protocol is safe and meets the design goals of the proposed systems. Thus, it can be stated that the security goals laid out in the HLPSL modelling are achieved. The result statistics obtained after simulation using AVISPA is illustrated in the Figure 3. The proposed authentication approach is simulated

TABLE III
COMPARISON OF SECURITY AND FUNCTIONALITY FEATURES

Security features	[18]	[23]	[26]	[25]	[24]	[29]	[27]	[28]	[31]	[30]	[34]	Proposed
Man in the middle attack	●	○	●	●	○	○	●	○	●	●	●	●
Impersonation attack	○	○	○	●	○	○	●	○	●	●	○	●
DoS attack	○	●	●	○	●	○	○	●	○	○	○	●
Replay Attack	●	●	●	○	●	○	●	●	●	○	●	●
Session Key Disclosure Attack	○	○	○	○	●	○	●	○	○	○	○	●
Offline password attack	○	○	○	●	○	○	○	○	○	○	○	●
Prevention of Insider Attack	○	○	○	○	○	●	○	○	○	●	○	●
Eavesdropping Attack	○	○	○	○	○	○	○	○	○	○	○	●
Message authentication	●	●	○	●	●	○	●	●	●	○	●	●
Forward secrecy	○	○	○	○	○	○	●	○	●	○	●	●
Privacy of customer	○	○	○	○	●	●	●	●	●	○	●	●
Mutual authentication	●	●	●	●	●	○	●	●	●	●	●	●
Session key security	○	○	○	○	○	○	●	○	○	○	●	●
Traceability	○	●	○	●	●	●	○	○	○	●	●	●
Perfect forward security	○	●	○	●	●	○	●	○	●	●	●	●
Unlinkability	○	●	○	○	●	○	○	●	○	○	●	●
Anonymity	●	●	●	●	●	●	○	○	●	●	●	●
Using ROR Model	○	●	○	●	●	○	●	●	●	○	●	●
Key freshness	○	○	○	●	●	○	○	●	●	○	○	●
Session key agreement	○	●	○	●	●	○	●	●	●	●	●	●

Note ⇒ ● Demonstrates the capability to secure against attacks or fulfill the specified property; and ○ Lacks the ability to secure against said attacks or not fulfill the specified property.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/v2g.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.12s
  visitedNodes: 4 nodes
  depth: 2 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/v2g.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.04 seconds
  Computation: 0.00 seconds
```

Fig. 3. Results of AVISPA using OFMC and CL-AtSe.

through CL-AtSe and OFMC backends. As per the result statistics in Figure 3, 128 nodes are visited through the OFMC backends with 4 plies and 1.61s search time. The OFMC backend failed to trace any attack under the DY threat model. Similarly, 5 states are analyzed by CL-AtSE backend with 0.24 seconds translation time. The CL-AtSE backend is also failed to trace any attack under DY threat model. As per the simulation results analysis, the proposed approach is secure under the threat model.

VI. PERFORMANCE ANALYSIS

This subsection conducts a comparative analysis of the proposed authentication scheme and existing methods, focusing on security and functional capabilities, computational cost, communication overhead, and energy efficiency, and outlines the merits and limitations of each approach.

A. Comparison of Security And Functionality Features

A comparison of the proposed security framework with existing authentication schemes [18], [23], [24], [25], [26], [27], [28], [29], [30], [34] highlights differences in meeting security and functionality requirements. The proposed solution is built to comprehensively address security challenges in V2G networks and is designed to be robust against known attacks. As shown in Table III, it improves upon current methods in both security performance and functional reliability. The protocol ensures mutual authentication and secure key establishment, while upholding critical properties such as forward secrecy, user confidentiality, and fairness in session key negotiation.

B. Computation Cost Comparison

To implement and evaluate our system we selected two distinct platforms one for the User Interface (UI) and another for the CS/USP server based on practical considerations such as performance, compatibility, and ease of deployment. The UI was developed and tested on a Lenovo Zuk Z1 smartphone. This device is powered by a quad-core 2.5 GHz processor and equipped with 4 GB of RAM, providing sufficient processing power for responsive user interactions. The device runs on Android OS version 5.1.2, ensuring compatibility with a wide range of mobile development frameworks and tools. This configuration was chosen to simulate real-world usage conditions on a mid-range smartphone. The CS/USP server component was deployed on a virtual machine hosted on an HP E8300 workstation, featuring an Intel Core i5 processor running at 2.93 GHz and 4 GB of RAM. The virtual environment operates on Ubuntu Linux version 16.11, providing a stable and widely supported open-source operating system for server-side application development and deployment. This setup facilitates scalability and resource management while maintaining consistency across test environments. Table IV presents the execution times and descriptions of various operations carried out by the proposed protocol and its counterparts,

TABLE IV
EXECUTION TIME OF CRYPTOGRAPHIC PRIMITIVES IN MILLISECOND

Operation	Description	User Cost(ms)	Server Cost(ms)
T_h	One-way hash function	0.019	0.012
T_{ecm}	ECC scalar point multiplication	10.235	5.387
$T_{enc/dec}$	Symmetric encryption /decryption	0.063	0.048
T_{eca}	ECC-based point addition	5.012	2.002
T_{exp}	Modular exponentiation operation	8.341	3.362
T_{bp}	Bilinear pairing operation	13.662	7.318

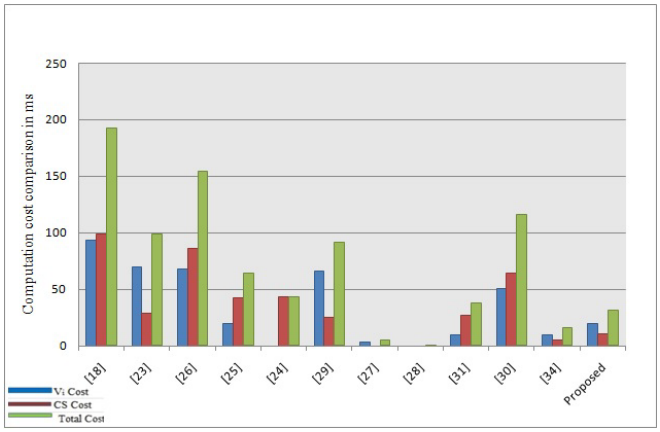

Fig. 4. Comparative analysis of computational costs.

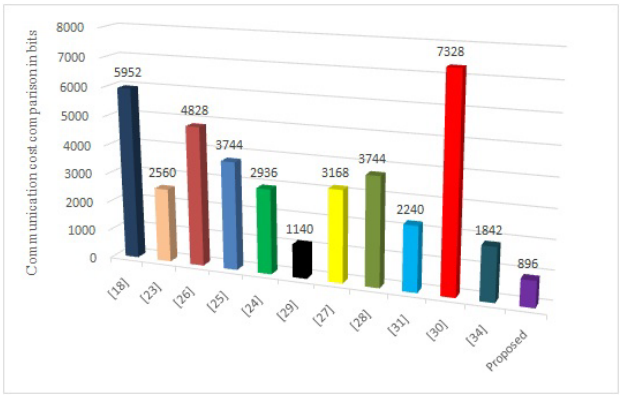

Fig. 5. Comparative analysis of communication costs.

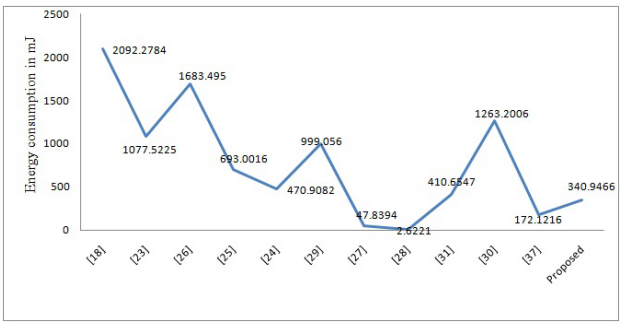

Fig. 6. Comparative analysis of energy consumption.

based on the findings reported in [37]. As illustrated in Table V and the accompanying Figure 4, the comparative analysis of computational costs indicates that our proposed protocol performs more efficiently than existing schemes in similar contexts. Moreover, the comparison underscores that our protocol not only achieves enhanced security and functional capabilities but also maintains lower computational cost relative to other existing competing protocols in same environment, as evidenced in Table V.

C. Communication Cost Comparison

In Table VI, we present a detailed evaluation of the communication costs of the proposed framework in comparison with related frameworks within the same application domain [18], [23], [24], [25], [26], [27], [28], [29], [30], [34]. The comparison is based on metrics such as the number of communication rounds, message sizes, and overall data exchanged during protocol execution. The results demonstrate the communication efficiency of the proposed scheme and its practicality in environments where minimizing overhead is essential. Further, The communication cost was calculated as shown here as assumed that identity, point multiplication and random numbers require 160 bits each. Additionally, one way secure hash function and SignCrypt/UnsignCrypt and encryption/decryption take 256 bits [37]. Therefore, it can be concluded that the proposed protocol achieves significantly lower communication costs compared to most previously developed schemes, except for a few protocols that either lack adequate security or incur higher computational costs.

D. Energy Consumption

Energy consumption in the communication system is defined as the total amount of energy expended during its operational processes. This parameter is quantitatively measured in millijoules (mJ) to evaluate the system's energy efficiency. Energy consumption is determined as $EC_{et} = TC2 * P_p$, where P_p [41] is the maximal processing power, $TC2$ is the total computational cost, and EC_{et} is the energy consumed. Table VI shows the total energy consumption of our designed protocol and other related protocols [18], [23], [24], [25], [26], [27], [28], [29], [30], [34]. Our proposed protocol used significantly less energy than [18], [23], [24], [25], [26], [29], and [30], and slightly more energy than [27], [28], and [34]. However, [27], [28], [34] are vulnerable to various security attacks and do not satisfies the security properties in an environment of V2G which is provided in Table III. Moreover, Figure 6 quantitatively compares the energy efficiency of the proposed protocol and other existing protocols operating under similar environmental, highlighting the improvements achieved in reducing energy consumption.

VII. ASSUMPTIONS AND LIMITATIONS

This section provide the details key assumptions and the associated limitations are as follows:

A. Key Assumptions

- **Secure channel:** The communication between the V_i and CS is assumed to be secure and reliable by utilizing the session shared key between them. This is a standard assumption in key agreement and authentication schemes.
- **Clock synchronization:** The protocol is based on loose time synchronization V_i and CS within the maximum $\triangle t$

TABLE V
COMPUTATION COST COMPARISON

Protocols	**Vehicle User Costs**	**Charging Station Costs**	**Total cost(ms)**
Saxena and Choi [18]	$6T_h + T_{bp} + T_{ecm} + 2T_{eca} + T_{exp} \cong 93.448$	$11T_h + 2T_{bp} + 5T_{ecm} + 17T_{exp} \cong 98.857$	$\cong 192.305$
Li et al. [23]	$10T_h + T_{bp} + 5T_{ecm} + T_{eca} \cong 70.039$	$11T_h + T_{bp} + 4T_{ecm} \cong 28.998$	$\cong 99.037$
Roman et al. [26]	$8T_h + 3T_{bp} + 5T_{ecm} + T_{asm_{enc/dec}} \cong 68.052$	$15T_h + 3T_{bp} + 9T_{ecm} + 8T_{eca} + T_{asm_{enc/dec}} \cong 86.681$	$\cong 154.733$
Garg et al. [25]	$3T_h + 2T_{ecm} \cong 20.527$	$6T_h + 8T_{ecm} \cong 43.168$	$\cong 63.695$
Gope and Sikdar [24]	$6T_h \cong 0.114$	$6T_h + 8T_{ecm} \cong 43.168$	$\cong 43.282$
Su et al. [29]	$2T_h + 5T_{ecm} + 3T_{eca} \cong 66.249$	$2T_h + 4T_{ecm} + 2T_{eca} \cong 25.576$	$\cong 91.825$
Bansal et al. [27]	$4T_h + 2T_{asm_{enc/dec}} \cong 4.145$	$5T_h + 4T_{asm_{enc/dec}} \cong 0.252$	$\cong 4.397$
Irshad et al. [28]	$7T_h \cong 0.133$	$9T_h \cong 0.108$	$\cong 0.241$
Ahmad et al. [31]	$4T_h + 2T_{asm_{enc/dec}} + T_{ecm} \cong 10.437$	$7T_h + 6T_{asm_{enc/dec}} + 5T_{ecm} \cong 27.307$	$\cong 37.744$
Kumar et al. [30]	$7T_h + 5T_{ecm} \cong 51.327$	$11T_h + 12T_{ecm} \cong 64.776$	$\cong 116.103$
Shamshad et al. [34]	$6T_h + T_{ecm} \cong 10.349$	$7T_h + T_{ecm} \cong 5.471$	$\cong 15.82$
Proposed	$3T_h + 2T_{ecm} \cong 20.527$	$3T_h + 2T_{ecm} \cong 10.81$	$\cong 31.337$

TABLE VI
COMPARATIVE ANALYSIS OF COMMUNICATION COSTS IN BITS AND ENERGY CONSUMPTION(MJ)

Scheme	**CC**	**EC(mJ)**
Saxena and Choi [18]	5952	2092.2784
Li et al. [23]	2560	1077.5225
Roman et al. [26]	4828	1683.4950
Garg et al. [25]	3744	693.0016
Gope and Sikdar [24]	2936	470.9082
Su et al. [29]	1140	999.056
Bansal et al. [27]	3168	47.8394
Irshad et al. [28]	3744	2.6221
Ahmad et al. [31]	2240	410.6547
Kumar et al. [30]	7328	1263.2006
Shamshad et al. [34]	1842	172.1216
Proposed	896	340.9466

Note:CC: Communication Cost in bits; EC: Energy Consumption

to stop replay attacks. Significant clock drift beyond this window will trigger a fallback to full authentication.

- **Cryptographic primitives:** The security proofs assume the underlying cryptographic primitives such as SHA-256, AES-256, ECC are secure and that hash functions behave as ideal random oracles.

B. Limitations

- **Initial registration overhead:** The one-time ECC-based registration, while efficient in the long run, introduces a higher initial computational overhead compared to purely symmetric-key protocols. In scenarios with extremely high device churn where devices are constantly registering and de-registering, this overhead could become a bottleneck, requiring load-balanced server infrastructure.
- **Dependence on user password:** The security of credentials stored on the device hinges on the strength of the user chosen password. While we recommend a complexity policy, a weak password remains a vulnerability point for a stolen device attack if the tamper-resistant hardware is compromised.
- **Quantum computing threat:** Like most current classical cryptographic protocols, the security of our protocol is not designed to be resilient against attacks from large scale fault tolerant quantum computers. In a post-quantum future, the ECC and symmetric cryptographic primitives would need to be replaced with quantum resistant alternatives.

VIII. CONCLUSION

In this article, we propose a Vehicle-to-Grid authentication scheme that prioritizes energy efficiency, in addition to providing security and privacy. The security of the proposed scheme is demonstrated in the formal random-oracle model and with the automated tool AVISPA. The article also provides an informal discussion on the security features offered by the proposed scheme. The comprehensive comparative performance analysis reveals that the proposed protocol achieves significantly lower computational and communication costs than some existing protocols. Hence, the proposed protocol presents a lightweight, efficient, and secure solution, making it highly suitable for real-world deployment in a V2G environment. Referring to the future work, we suggest extending the protocol for V2G networks with quantum-resistant security mechanisms.

ACKNOWLEDGMENT

The authors, therefore, acknowledge with thanks DSR for the technical and financial support.

REFERENCES

[1] C. C. Chan, "The state of the art of electric, hybrid, and fuel cell vehicles," *Proc. IEEE*, vol. 95, no. 4, pp. 704–718, Apr. 2007.

[2] G. Lopez, Y. Pourjamal, and C. Breyer, "Paving the way towards a sustainable future or lagging behind? An ex-post analysis of the international energy agency's world energy outlook," *Renew. Sustain. Energy Rev.*, vol. 212, Apr. 2025, Art. no. 115371.

[3] W. Kempton and S. E. Letendre, "Electric vehicles as a new power source for electric utilities," *Transp. Res. D, Transp. Environ.*, vol. 2, no. 3, pp. 157–175, Sep. 1997.

[4] D. B. Richardson, "Electric vehicles and the electric grid: A review of modeling approaches, impacts, and renewable energy integration," *Renew. Sustain. Energy Rev.*, vol. 19, pp. 247–254, Mar. 2013.

[5] K. Feeney, D. Brass, D. Kua, A. Yamamoto, E. Tourneboeuf, and D. Adams. (2011). *Impact of Electric Vehicles and Natural Gas Vehicles on the Energy Markets*. [Online]. Available: https://mpra.ub.uni-muenchen.de/58388/

[6] Y. Dashora, J. W. Barnes, R. S. Pillai, T. Combs, and M. Hilliard, "Optimized energy management for large organizations utilizing an on-site PHEV fleet, storage devices and renewable electricity generation," *Energy Syst.*, vol. 3, no. 2, pp. 133–151, Jun. 2012.

[7] S. Agrawal and P. Ahlawat, "A survey on the authentication techniques in Internet of Things," in *Proc. IEEE Int. Students' Conf. Elect., Electron. Comput. Sci. (SCEECS)*, Feb. 2020, pp. 1–5.

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

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

[10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2004, pp. 523–540.

[11] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[12] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

[13] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 707–714, Dec. 2011.

[14] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.

[15] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution scheme proposed by Xia and Wang," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1613–1614, Sep. 2013.

[16] J. Chen, Y. Zhang, and W. Su, "An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-grid (V2G) networks," *China Commun.*, vol. 12, no. 3, pp. 9–19, Mar. 2015.

[17] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[18] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1438–1452, Jul. 2016.

[19] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[20] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[21] A. Abdallah and X. S. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615–2629, Mar. 2017.

[22] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018.

[23] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K.-R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Gener. Comput. Syst.*, vol. 83, pp. 607–618, Jun. 2018.

[24] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6607–6618, Nov. 2019.

[25] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. P. C. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[26] L. F. A. Roman, P. R. L. Gondim, and J. Lloret, "Pairing-based authentication protocol for V2G networks in smart grid," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101745.

[27] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.

[28] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4425–4435, Jul. 2020.

[29] Y. Su, G. Shen, and M. Zhang, "A novel privacy-preserving authentication scheme for V2G networks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1963–1971, Jun. 2020.

[30] V. Sureshkumar, S. Mugunthan, and R. Amin, "An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network," *Peer-Peer Netw. Appl.*, vol. 15, no. 5, pp. 2347–2363, Sep. 2022.

[31] S. Ahmed et al., "Signcryption based authenticated and key exchange protocol for EI-based V2G environment," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5290–5298, Nov. 2021.

[32] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, "ABRIS: Anonymous blockchain based revocable and integrity preservation scheme for vehicle to grid network," *Energy Rep.*, vol. 8, pp. 9331–9343, Nov. 2022.

[33] W. Hou, Y. Sun, D. Li, Z. Guan, and J. Liu, "Lightweight and privacy-preserving charging reservation authentication protocol for 5G-V2G," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7871–7883, Jun. 2023.

[34] S. Shamshad, K. Mahmood, U. Shamshad, I. Hussain, S. Hussain, and A. K. Das, "A provably secure and lightweight access control protocol for EI-based vehicle to grid environment," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16650–16657, Sep. 2023.

[35] V. Sureshkumar, P. Chinnaraj, P. Saravanan, R. Amin, and J. J. P. C. Rodrigues, "Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3470–3479, Apr. 2022.

[36] A. G. Reddy, P. R. Babu, V. Odelu, L. Wang, and S. A. P. Kumar, "V2G-auth: Lightweight authentication and key agreement protocol for V2G environment leveraging physically unclonable functions," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 1, pp. 66–78, 2023.

[37] S. Yu and K. Park, "PUF-based robust and anonymous authentication and key establishment scheme for V2G networks," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 15450–15464, May 2024.

[38] S. Ahmed and M. H. Anisi, "Optimizing V2G dynamics: An AI-enhanced secure protocol for energy management in industrial cyber-physical systems," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 312–320, 2024.

[39] P. Xu, X. Wang, and M. Chen, "A secure authentication and key exchange protocol for vehicles to infrastructure network," *Int. J. Comput. Intell. Syst.*, vol. 18, no. 1, p. 26, Feb. 2025.

[40] A. Armando et al., "The AVISPA tool for the automated validation of internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2005, doi: 10.1007/11513988_27.

[41] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012.