Received 18 April 2024, accepted 8 May 2024, date of publication 13 May 2024, date of current version 23 May 2024.
Digital Object Identifier 10.1109/ACCESS.2024.3400517

RESEARCH ARTICLE

Mutual and Batch Authentication With Conditional Privacy-Preserving Scheme for $V2G$ Communication System

JEGADEESAN SUBRAMANI[1], AZEES MARIA[2], (Member, IEEE), ARUN SEKAR RAJASEKARAN[3], (Member, IEEE), AND BABJI PRASAD CHAPA[4]
[1]Department of Electronics and Communication Engineering, M. Kumarasamy College of Engineering, Karur 639113, India
[2]School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh 522237, India
[3]Department of Electronics and Communication Engineering, SR University, Warangal, Telangana 506371, India
[4]Department of Electronics and Communication Engineering, GMR Institute of Technology, Vizianagaram, Andhra Pradesh 532127, India
Corresponding author: Azees Maria (azeesmm@gmail.com)

This work was supported by VIT-AP University, Amaravati, Andhra Pradesh, India.

ABSTRACT The increasing adoption of intelligent Electric Vehicles (EVs) in the realm of transportation has raised significant concerns pertaining to security aspects within the Vehicle-to-Grid ($V2G$) communication system. This includes issues related to authentication, integrity, confidentiality, privacy, and the effective tracking of EVs. While numerous researchers have proposed solutions to address these security challenges, the existing schemes often exhibit a considerable demand for computational and communication resources. This renders them impractical for resource-limited $V2G$ setups operating within the Internet-of-Things (IoT) framework. To address these limitations, this paper introduces an energy-efficient mutual and batch authentication scheme tailored specifically for $V2G$ communication systems within the IoT paradigm. Through a meticulous security and performance analysis, our proposed scheme demonstrates its proficiency in providing essential security features, including robust authentication and privacy safeguards, while significantly minimizing both computational and communication complexity. The outcomes of our analysis affirm that the proposed approach is well-suited for the unique constraints of IoT-based $V2G$ communication systems, offering a balanced and resource-efficient solution to enhance overall security and performance.

INDEX TERMS Authentication, confidentiality, electric vehicle, integrity, privacy, vehicle-to-grid communication.

I. INTRODUCTION

In recent years, the rapid advancements in wireless technologies and the proliferation of the Industrial Internet of Things ($IIoT$) have ushered in transformative changes across various industries. The widespread implementation of $IIoT$ across various sectors, including healthcare, transportation, and Smart Grid (SG), highlight its increasing significance [1]. Within this context, SG emerge as a pivotal driver of $IIoT$, leveraging interconnected devices such as smart meters, sensors, and aggregators over the Internet [1].

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

According to a report from Kyrio, the IoT sector's utilization in the utility industry is projected to reach $15 billion by 2024 [2]. The primary objective of SG is to optimize energy utilization while minimizing electricity losses. To achieve this, surplus electricity generated during periods of high-power generation is stored in energy storage devices like fuel cells, flywheels, and EVs. Subsequently, this stored energy can be reintegrated into the SG during periods of high demand. With their growing popularity, EVs emerge as promising storage devices, providing reliable units with minimal energy loss.

Moreover, the rapid charging and discharging capabilities of EV batteries make them superior to adjusting the generation levels of traditional power sources to match current electricity demand. Coined as $V2G$ link, this bidirectional communication between *EVs* and the power grid facilitates the efficient exchange of electricity [2], [3], [4]. This bidirectional interaction not only optimizes energy usage but also generates valuable data for predicting pricing, load forecasting, and optimizing energy consumption scheduling [4].

Additionally, communication within the $V2G$ system extends beyond the power grid to encompass interactions between *EVs* and Charging Stations (*CS*), all conducted through a wireless medium. The high mobility of *EVs* shortens the communication time between them, necessitating efficient authentication and privacy preservation mechanisms. Many existing authentication schemes [5], [6], [7], [8] involve time-consuming processes such as certificate revocation list verification and signature verification by vehicles to authenticate received information, aiming to prevent malicious entry. Upon examining the challenges posed by current authentication schemes, it becomes clear that there is a pressing need for streamlined and resource-efficient approaches to enhance the effectiveness of $V2G$ communication systems.

Incorporating $V2G$ communication is essential within the framework of *SG* and the broader context of the $IIoT$. To begin with, $V2G$ communication plays a pivotal role in efficiently managing surplus electricity generated during peak periods by storing it in *EV* batteries. This stored energy can then be seamlessly reintegrated into the grid during times of heightened demand, thereby bolstering grid stability and minimizing energy wastage.

Furthermore, $V2G$ communication facilitates the seamless integration of renewable energy sources into the grid by providing a mechanism to store excess energy from intermittent sources like solar and wind power. This capability ensures a consistent and dependable energy supply, contributing to grid reliability and stability.

Moreover, $V2G$ communication enables *EVs* to provide essential grid services such as frequency regulation and voltage support, thereby enhancing the overall stability and reliability of the grid as it transitions towards a more decentralized and renewable-based system.

Additionally, $V2G$ communication yields valuable insights into electricity consumption patterns, charging behaviors, and grid conditions. This data can be leveraged for accurate load forecasting, optimization of pricing strategies, and informed infrastructure planning, ultimately enhancing the efficiency and effectiveness of the grid.

A. OUR CONTRIBUTIONS

The following is the key objective of the proposed scheme.

- Introduce an energy-efficient authentication method for *EVs*, ensuring anonymous authentication in $V2G$ communication.
- Implement anonymous signature verification for robust data integrity within the $V2G$ system.
- Establish conditional privacy to reveal real identities of mischievous $V2G$ users, promoting accountability.
- Propose an energy-efficient batch authentication scheme for multiple *EVs*, reducing authentication time and computational burden.

The remaining sections of our work are organized as follows: Section II offers an extensive review of related literature. Section III outlines the system model, delves into the core concepts of our proposed approach, and establishes the attack model. Section IV provides an in-depth description of our proposed authentication and privacy-preserving system. Section V focuses on the assessment of the security resilience of our approach, while Section VI evaluates its performance efficiency. Lastly, Section VII presents the conclusions derived from our research.

II. RELATED WORKS

The evolving field of $V2G$ communication, situated at the intersection of *EV* technology and *SG* systems, has witnessed substantial research efforts in recent years. In the context of smart cities, Firoz Khan et al.'s work [8] lays a foundational perspective on cyber-physical systems, providing a broad understanding of the smart city paradigm and its relevance to the $V2G$ framework. This contextualizes $V2G$ as an integral component of the broader vision for intelligent urban infrastructure.

Security and privacy are paramount considerations in $V2G$ communication implementation. Nicanfar and Leung's Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) protocol [9] stands out as a notable contribution, introducing a secure and multi-layered approach to key exchange in *SG* systems. This protocol addresses potential vulnerabilities associated with cryptographic key management, thereby enhancing the security of $V2G$ communication.

Wu and Zhou's study [10] focuses on exploring fault-tolerant and scalable key management for *SG*, which is a crucial aspect in ensuring the integrity and confidentiality of communication in $V2G$ systems. Additionally, Xia and Wang [11] delve into secure key distribution mechanisms, laying the groundwork for cryptographic approaches within $V2G$ networks.

Building upon these foundational studies, Park et al. [12] identify security weaknesses in key distribution proposed by Xia and Wang, prompting further investigations. In response, Tsai and Lo [13] propose a secure anonymous key distribution scheme tailored for *SG*, adding an additional layer of privacy to $V2G$ communication. Odelu et al.'s work [14] introduces a provably secure authenticated key agreement scheme, contributing to the robustness of cryptographic mechanisms in $V2G$ networks.

Privacy preservation is emerging as a critical focus in $V2G$ communication. Liu et al. [15] advocate for role-dependent privacy strategies, while Yang et al.'s [16] proposed privacy-preserving communication architecture for $V2G$ networks add another layer of privacy consideration.

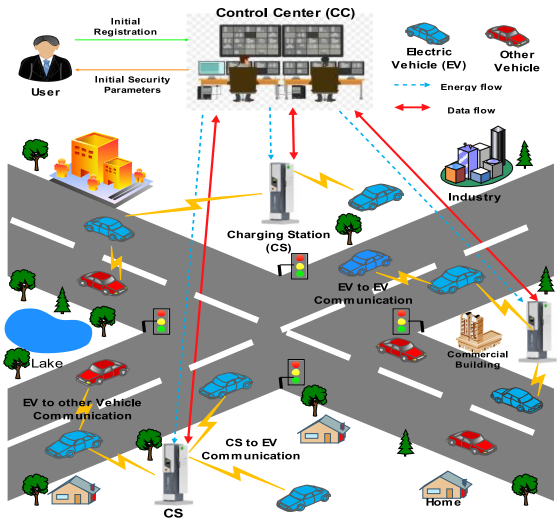


FIGURE 1. System model.

TABLE 1. Notations and description.

Notation	Description
EV_{pr_i}	Private key of EV_i
EV_{pu_i}	Public key of EV_i
TPD	Tamper-proof device
BAK_i	Batch authentication key for EV_i
BTK_i	Batch tracking key for EV_i
FID_{EV_i}	Fake identities of EV_i
FID_{CS_i}	Fake identities of CS_i
CS_{pr_i}	Private key of CS_i
CS_{pu_i}	Public key of CS_i
CBK_i	Batch authentication key for CS_i
CTK_i	Batch tracking key for CS_i
OTC	One-time challenger

This architecture ensures precise reward distribution while maintaining user confidentiality.

Beyond cryptographic considerations, several studies contribute insights into broader aspects of $V2G$ communication. Kong et al. [17] conduct a thorough analysis of handover latency, shedding light on critical aspects of network-based localized mobility management protocols. Jegadeesan et al.'s [18] work on trajectory privacy-preserving schemes adds a layer of confidentiality to the mobility patterns associated with $V2G$ communication.

In the realm of tooling, Lynn's PBC library [19] and the Cygwin platform [20] are fundamental resources for cryptographic implementations in various studies. These tools provide a robust foundation for researchers and practitioners working on cryptographic aspects of $V2G$ communication. Authentication schemes for renewable energy-based SG environments are explored by Wazid et al. [21], Jo et al. [22], and Kaur et al. [23]. Each study contributes unique perspectives on efficient and secure approaches to user authentication, catering to the specific requirements of $V2G$ systems.

Extending the discussion to $V2G$ connections in SG, Jegadeesan et al.'s [23] work on a secure, lightweight, and privacy-preserving authentication scheme adds valuable insights into the challenges and potential solutions in the authentication domain. The landscape of $V2G$ communication is not confined solely to the SG context. Subramani et al.'s [24] efficient anonymous authentication scheme for automatic dependent surveillance-broadcast systems and Jegadeesan et al.'s [25] privacy-preserving anonymous authentication scheme for human predictive online education systems highlight the adaptability of privacy-centric approaches across diverse domains.

In conclusion, this comprehensive literature survey highlights the multidimensional nature of research in $V2G$ communication. From cryptographic protocols and privacy preservation strategies to authentication mechanisms and broader implications, the studies presented provide a comprehensive overview of the current state of $V2G$ communication. These foundational works set the stage for continued exploration and innovation in this dynamic and rapidly evolving field.

III. SYSTEM MODEL, PRELIMINARIES, AND ATTACK MODEL

A. SYSTEM MODEL

The proposed scheme's comprehensive system model is illustrated in Figure 1, comprising a Control Center (CC), Charging Stations (CS), and Electric Vehicles (EVs) equipped with Onboard Units ($OBUs$). CSs establish a connection with CC through the Internet using a backbone network [15]. An explanation of the symbols used in the proposed approach is provided in Table 1.

1) CONTROL CENTER (CC)

CC serves as the trusted administrative hub of the $V2G$ communication system, responsible for procuring electricity from various vendors and distributing it to strategically located CSs across the country. Both CSs and EVs must register with CC before participating in the $V2G$ communication system. This work assumes a distinct CC for each state, facilitating efficient EV identification validation when traveling across states. The CCs are interconnected through an IoT architecture [17].

2) CHARGING STATION (CS)

Strategically positioned in parking areas or along roadsides, CSs are maintained by government or private agencies. The spacing between CSs is determined by vehicle density. EV users can charge or discharge their EV batteries at any CS, with the electricity rate subject to change based on the $CS's$ location. Although the CSs are considered partially trusted in this work, potential compromises could lead to the exposure of sensitive information. To mitigate hardware attacks on CSs, continuous monitoring is implemented through surveillance cameras.

3) ELECTRIC VEHICLE (*EV*)

All *EVs* are equipped with *OBUs* to facilitate communication with *CSs* and other *EVs*, ensuring seamless travel. Each *OBU* incorporates a tamper-proof device (*TPD*) for secure storage of secret keys, event data recorder, and a global positioning system to securely report event and location-based information. *EVs* can simultaneously access *CSs* for charging or discharging services. Additionally, *OBUs* transmit traffic-related information to other vehicles, enhancing traffic management.

B. BILEAR PAIRING

Let G_1, G_2, and G_T be the multiplicative cyclic groups of order p, where p stands for larger prime number. Let the generator of G_1 is g_1 and the generator of G_2 is g_2. Assume that G_1, G_2, and G_T are equipped with pairing. $e : G_1 \times G_2 \rightarrow G_T$ is a bilinear map, and it should satisfy the following properties.

1) BILINEAR

$e\left(g_1^x, g_2^y\right) = e(g_1, g_2)^{xy}$ for all $g_1 \in G_1, g_2 \in G_2$ and $x, y \in Z_p^*$, Where $Z_p^* = [1, 2, \ldots, (p-1)]$.

2) NON-DEGENERACY

$e(g_1, g_2) \neq 1G_T$.

3) COMPUTABILITY

There is an efficient approach for quickly computing the bilinear map $e : G_1 \times G_2 \rightarrow G_T$.

The isomorphism is denoted by ψ, and the $\psi : G_2 \rightarrow G_1$ is required basically.

C. ATTACK MODEL

In the proposed scheme, any network element deviating from its intended functions or exhibiting misbehavior is considered an adversary. Given the inherent openness of wireless communications, the attack model encompasses both internal and external adversaries.

1) EXTERNAL ADVERSARIES

External attackers, as network outsiders, have the capability to intercept communications and scrutinize information exchanged between system entities. This enables them to ascertain identities, monitor locations, and potentially disclose the contents of transmitted information if in possession of the requisite decryption keys. Consequently, external adversaries can execute various attacks such as "man-in-the-middle," "replay," "message manipulation," and "impersonation."

2) INTERNAL ADVERSARIES

Internal attackers include network components or malfunctioning *EVs* engaging in illicit activities within the system. A misbehaving EV, for instance, may initiate a repudiation attack to evade its obligations and exploit services for unauthorized purposes. These internal adversaries pose a threat to the system's integrity and proper functioning, necessitating robust security measures to counteract potential attacks.

IV. PROPOSED SCHEME

The proposed scheme comprises six sections, including system initialization, user registration, key distribution, mutual authentication, conditional privacy preservation, and batch authentication.

A. SYSTEM INITIALIZATION

Initially, the $\boldsymbol{CC}$ chooses random numbers $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{Z_p^*}$ as its main secret key, and it is used to calculate the registered user's public key by using their private keys. Next, the $\boldsymbol{CC}$ selects $\boldsymbol{CC_{pr}} \in \boldsymbol{Z_p^*}$ as its private key and calculates $\boldsymbol{CC_{pu}} = \boldsymbol{g_1^{CC_{pr}+v}}$ as its public key. After that, the $\boldsymbol{CC}$ chooses $\boldsymbol{H} : \boldsymbol{\{0, 1\}^*} \rightarrow \boldsymbol{Z_p^*}$ as a secure cryptographic hash function. Finally, the $\boldsymbol{CC}$ announces the proposed system parameters $\boldsymbol{param} = (\boldsymbol{p}, \boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{G_1}, \boldsymbol{G_2}, \boldsymbol{e}, \boldsymbol{CC_{pu}}, \boldsymbol{H})$ to the public.

B. REGISTRATION

Step 1: Initially, the EV_i submits all the necessary documents to the CC. Next, the CC picks a random number $EV_{pr_i} \in Z_p^*$ as an EV_i private key and calculates the corresponding EV_i public-key as

$$EV_{pu_i} = g_1^{EV_{pr_i}+v} \tag{1}$$

After that, the EV_i needs to register his/her tamper-proof device (*TPD*) with the CC. During the *TPD* registration, the CC assigns the credential as $cr_i = g_1^{u+v}$, and it calculates the *TPD* activation key as

$$ak_i = g_1^{EV_i+u+v+CC_{pr}} \tag{2}$$

Using this credential and the activation key, the EV_i activates *TPD* and derives its own EV_{pr_i} and EV_{pu_i}. To find the cr_i and ak_i during the key distribution phase, the CC calculates the $DE_i = cr_i * EV_{pu_i}$ as a dual encryption key.

Step 2: The CC assigns

$$VI_{EV_i} = EV_{pu_i}^u * g_1^u \tag{3}$$

as a $V2G$ communication system user identity (VI_{EV_i}) to each EV_i.

Step 3: To authenticate a batch of requests/messages from EV_i in a single time, the CC needs to calculate the batch authentication key as

$$BAK_i = g_1^{CC_{pr}+v+EV_{pr_i}} \tag{4}$$

Also, the CC generates the batch tracking key as

$$BTK_i = g_1^{-CC_{pr}-v} \tag{5}$$

to trace the misbehaving EV_i in $V2G$ communication system.

Step 4: The CC assigns a unique identity to every EV_i user as UID_{EV_i} during the registration. Next, the CC calculates fake identities (FID_{EV_i}) to all EV_i users. To calculate fake identities, the CC first selects the random number $f_1 \in Z_p^*$ and calculates the fake identity as

$$FID_{EV_i} = g_1^{f_1+CC_{pr}+v} modp \tag{6}$$

Likewise, the CC calculates the fake identities for CSs as

$$FID_{CS_i} = g_1^{F_1+CC_{pr}+v} \tag{7}$$

The mapping of UID_{EV_i} to FID_{EV_i} was done only in the CC. The fake identities are generated for every EV_i user to validate the message source. If an adversary obtains these identities, there is no way to know about the real identity of EV_i user or CSs. Therefore, the adversary cannot reveal the privacy of the EV_i user or CSs. The CC maintains the details of FID_{EV_i}, UID_{EV_i}, $EV_{pu_i}^{u*v}$ in the tracing table. In case of dispute, the CC can revoke the EV_i from the $V2G$ communication system.

Step 5: The CC pre-store the values of EV_{pr_i} and EV_{pu_i} in every EV_i's TPD. The CC gives the values of FID_{EV_i}, cr_i, VI_{EV_i}, DE_i, and TI_i to corresponding EV_i users during the offline-mode registration process. Where $TI_i = g_1^{-f_1} modp$.

Step 6: In CS_i registration process, the CC picks the random number $CS_{pr_i} \in Z_p^*$ as CS_i private key and computes the CS_i public-key as

$$CS_{pu_i} = g_1^{CS_{pr_i}+u} \tag{8}$$

The CS_{pr_i} and CS_{pu_i} are used for mutual information exchange between the CS_i and CC.

Step 7: To authenticate the batch of requests/messages from the CSs, the CC computes the CS batch authentication key for every CS_i as

$$CBK_i = g_1^{CC_{pr}+v} \tag{9}$$

Also, the CC generates the batch tracking key as

$$CTK_i = g_1^{-CS_{pr}-v} \tag{10}$$

to trace the misbehaving CS_i in the $V2G$ communication system.

Step 8: The CC assigns $V2G$ communication system identity (VI_{CS_i}) for all the registered CS_i as

$$VI_{CS_i} = CS_{pu_i}^{v} * g_1^{v} \tag{11}$$

After that, the CC gives the VI_{CS_i} and ti_i values to the vehicle users, Where $ti_i = g_1^{-F_1} modp$.

Step 9: The CC maintains the values of FID_{CS_i}, $UID_{CS_i}, g_1^{v(1+CS_{pr_i})}$ in the tracing table. UID_{CS_i} is the CS_i unique identity and it is assigned by CC during the registration process. In case of dispute, CC can revoke the CS_i from the $V2G$ communication system.

C. SECURE TPD ACTIVATION

In this work, if EV_i wants to communicate with the other $V2G$ communication system entities, it is essential to derive the values of EV_{pr_i} and EV_{pu_i} from the TPD. TPD need to be activated to derive the values of EV_{pr_i} and EV_{pu_i}. To find the activation key, EV_i need to send its encrypted identification to CC with the help of CC_{pu} as $E_{CC_{pu}}(VI_{EV_i})$. The CC decrypts the received $E_{CC_{pu}}(VI_{EV_i})$ using it's CC_{pr} and calculates the secret information (SI) as

$$SI = cr_i * ak_i * EV_{pu_i} \tag{12}$$

Next, the CC sends the encrypted version of SI, $E_{cr_i}(SI)$ to the EV_i with the help of cr_i. The EV_i derive the TPD activation key (AK) by decrypting the value of $E_{cr_i}(SI)$ as follows.

$$ak_i = \frac{SI}{DE_i} = \frac{cr_i * ak_i * EV_{pu_i}}{cr_i * EV_{pu_i}} = ak_i \tag{13}$$

If both cr_i and ak_i are correct, the TPD will issue the EV_{pr_i} and EV_{pu_i} values to the EV_i user. Activation of TPD is not possible if $cr_i \neq ak_i$.

D. ANONYMOUS MUTUAL AUTHENTICATION

Mutual authentication among the EVs or EV to CS is done to communicate the (dis) charge request/response message and avoid communication with malicious EVs or CSs.

Step 1: The EV_i picks the random nonce r_i as its short-life private key from the set of R random nonce $r_1, r_2, \ldots, r_R \in Z_p^*$ and calculates $s_i = g_1^{r_i+EV_{pr_i}}$ as its corresponding public key. Where $i = 1, 2, \ldots, R$.

Step 2: The EV_i user calculates the short-life anonymous authentication certificate (OAC) for every s_i as follows.

The EV_i user picks the random nonce $a_1 \in Z_p^*$ and generates the one-time session keys $m_1 = g_1^{EV_{pr_i}}$ and $m_2 = g_1^{EV_{pr_i}+a_1}$. Then, the EV_i user calculates the one-time dummy session keys $\mathcal{M}_1 = g_1^{r_i-a_1}$ and $\mathcal{M}_2 = 1/g_1^{r_i}$. After that, the EV_i user generates the one-time challenger (OTC) as

$$OTC = H(CC_{pu} \parallel FID_{EV_i} \parallel s_i \parallel m_1 \parallel m_2) \tag{14}$$

After calculating the one-time dummy session keys and OTC, the EV_i user generates the OAC as

$$OAC = \{\mathcal{M}_1 \parallel \mathcal{M}_2 \parallel FID_{EV_i} \parallel OTC \parallel TI_i \tag{15}$$

Step 3: To preserve the anonymous request/response message (rrm_{EV_i}) integrity, the EV_i user generates the anonymous signature ($\mathbb{S}_{EV_i}$) as

$$\mathbb{S}_{EV_i} = g_2^{1/r_i+EV_{pr_i}+h} \tag{16}$$

After that, EV_i user sends the $rrm_{EV_i} \parallel \mathbb{S}_{EV_i} \parallel s_i \parallel OAC \parallel VI_{EV_i} \parallel TS_i$ to the CS or other EVs. Where TS_i denotes the current timestamp.

Step 4: After receiving $rrm_{EV_i} \parallel \mathbb{S}_{EV_i} \parallel s_i \parallel OAC \parallel VI_{EV_i} \parallel TS_i$ the CS or other EVs first verifies the integrity of the message by calculating,

$$e\left(s_i \times g_1^h, \mathbb{S}_{EV_i}\right) = e(g_1, g_2) \tag{17}$$

If it holds, the CS or other EVs accepts the rrm_{EV_i}. Otherwise, rrm_{EV_i} will be rejected immediately.

Step 5: After the integrity verification, the CS or other EVs verifies the TS_i to overcome the replay attack. The received TS_i is verified such that $\left|TS_j - TS_i\right| < \Delta T$, where ΔT is the agreed time delay between the communication entities in the $V2G$ communication systems. If it holds, the received rrm_{EV_i} is accepted. Otherwise, it will be rejected immediately.

Step 6: The CS or other EVs calculates $X_i = TI_i \times FID_{EV_i}$, $\mathbb{M}_1 = s_i \times \mathcal{M}_2$, and $\mathbb{M}_2 = s_i / \mathcal{M}_1$. Also, they calculate their one-time challenger (OTC') as

$$OTC' = H(X_i \parallel FID_{EV_i} \parallel s_i \parallel \mathbb{M}_1 \parallel \mathbb{M}_2) \quad (18)$$

After that, to authenticate the source of information, it checks the condition $OTC' = OTC$. If it holds, the received information is accepted. Otherwise, the received information will be rejected immediately.

E. CONDITIONAL PRIVACY PRESERVATION

If the received information rrm_{EV_i} from the EV_i, which has the identity of VI_{EV_i} has been disputed, then the CC can track the actual identity UID_{EV_i} efficiently by using its tracing table. Next, the CC can disclose the privacy of the EV_i, remove the EV_i from the $V2G$ communication system immediately and inform the same to other entities of the $V2G$ communication system. Similarly, the CC can track the misbehaving CS_i.

$$\frac{(VI_{EV_i})^v}{g_1^{u*v}} = \frac{(EV_{pu_i}^u * g_1^u)^v}{g_1^{u*v}} = \frac{EV_{pu_i}^{u*v} * g_1^{u*v}}{g_1^{u*v}} = EV_{pu_i}^{u*v} \quad (19)$$

F. ANONYMOUS BATCH AUTHENTICATION

A batch authentication scheme is introduced to expedite the authentication process by verifying multiple EVs simultaneously. The function of an anonymous batch authentication scheme is described as follows.

Step 1: The EV_i user first picks the random nonce $k_i \in Z_p^*$ as a short-life private key from the set of R random nonce $k_1, k_2, \ldots, k_R$, and calculates the public key $l_i = g_1^{k_i}$, where $i = 1, 2, 3, \ldots, k$. There are $'n' EVs$ $(EV_1, EV_2, \ldots, EV_n)$ under the specific CS, and the private keys for the $'n' EVs$ are given as $EV_{pr_1}, EV_{pr_2}, \ldots, EV_{pr_n}$.

Step 2: To receive a request/response message from the CS, every EV_i needs to generate the

$$A_i = g_1^{-EV_{pr_i} + k_i} \quad (20)$$

and

$$B_i = BAK_i \times A_i \quad (21)$$

Step 3: To maintain the integrity of l_i and B_i, the EV_i needs to calculate the hash value as $C_i = H(l_i \parallel B_i)$. After that, the EV_i calculates the tuple as $< l_i, B_i, C_i >$.

Step 4: The tuple value for a batch of $'n' EVs$ are given as $< l_1, B_1, C_1, BAK_1 >, < l_2, B_2, C_2, BAK_2 >, \ldots, < l_n, B_n, C_n, BAK_n >$.

Step 5: To verify the batch of tuples, first, the CS_i verify the integrity of l_i and B_i from every tuple by calculating $C_i = H(l_i \parallel B_i)$. After that CS_i collects $l = \prod_{i=1}^n l_n$ and $B = \prod_{i=1}^n B_n$.

Step 6: To anonymously authenticate the batch of EVs, the CS_i needs to verify the condition of

$$(CBK_i)^n = B / l \quad (22)$$

If it holds, CS_i authenticates the batch of EVs and sends the request/response message to EVs. Otherwise, it promptly terminates the connection.

V. SECURITY ANALYSIS

In this section, the proposed approach's security robustness is assessed considering various security threats.

A. IMPERSONATION ATTACK

In the suggested work, if an adversary ($\mathcal{A}$) needs to perform an impersonation attack, then he/she needs to find the one-time session key of EV_i and the EV_i private key issued by the CC during EV_i registration. However, $\mathcal{A}$ cannot compromise the user registration protocol since the $V2G$ communication system registration is done in offline mode at CC. The CC is considered a fully trusted one. Therefore, it is not possible for $\mathcal{A}$ to re-generate the session key. Also, the EV_{pu_i} is computed by CC depending on the rigidity of DLP [18], [26]. Hence, $\mathcal{A}$ cannot derive the random number u from the EV_{pu_i}.

B. MESSAGE MODIFICATION ATTACK

In the suggested work, the EV_i or CS_i user appends their signature to each piece of information to prevent the message modification attack. The EV_i or CS_i generates $\mathbb{S}_{EV_i}$ by using r_i and EV_{pr_i} or CS_{pr_i}. The specific EV_i or CS_i user only knows the values of private keys. Therefore, A cannot generate the EV_i or CS_i user signature without knowing the r_i and EV_{pr_i} or CS_{pr_i}. Even though A found the value of a r_i, it is unfeasible to generate the anonymous signature S_{EV_i}. Because the value of r_i is not a constant one, it will get changed periodically. Moreover, after receiving the request/response message from the EV_i or CS_i, the receiver will ensure the integrity of the received message by verifying the condition $e\left(s_i \times g_1^h, \mathbb{S}_{EV_i}\right) = e(g_1, g_2)$. If this condition is met, the receiver proceeds to verify the authentication certificate of EV_i or CS_i.

C. ANONYMOUS AUTHENTICATION

In this proposed work, every request/response message is attached with an anonymous authentication certificate before transmission to identify the source of information. The EV_i or CS_i user generates OAC by using the r_i and the EV_{pr_i} or CS_{pr_i}. The specific EV_i or CS_i user only knows the values of those private keys. Therefore, an $\mathcal{A}$ cannot generate the EV_i or CS_i user self-generated anonymous authentication certificate without finding r_i and EV_{pr_i} or CS_{pr_i}. Even though an $\mathcal{A}$ found the value of r_i, it is unfeasible to generate the anonymous signature S_{EV_i}. Because the value of r_i is not a constant one, it will get changed periodically. Moreover, to authenticate the source of information, it checks the condition $OTC' = OTC$. If it is true, the received data is accepted. Otherwise, the received information will be declined immediately.

D. REPLAY ATTACK

In this proposed work, the TS_i is added to each piece of information to prevent a replay attack. After receiving the information, the CS or other EVs verifies the TS_i. The received TS_i is verified such that $|TS_j - TS_i| < \Delta T$, where ΔT is the agreed time delay between the communication entities. If it holds, the received rrm_{EV_i} or rrm_{CS_i} is accepted.

E. FAKE INFORMATION ATTACK

In the suggested work, if A needs to transfer the false information to $V2G$ communication system users, then he/she wants to compute f_1 and FID_{EV_i} or FID_{CS_i}. The values of f_1 and FID_{EV_i} or FID_{CS_i} are calculated only by CC. To create fake identities, CC chooses a random number $f_1 \in Z_p^*$ and calculates the corresponding fake identity FID_{EV_i}. The mapping of UID_{EV_i} to FID_{EV_i} or UID_{CS_i} to FID_{CS_i} is done only at CC. Hence, it is difficult for A to derive f_1 or F_1 and v from FID_{EV_i}. The computational delay for finding v is $o[q^{\frac{1}{2}+o(1)} \log f]$. Here, f stands for the number of users registered in CC. Also, f_1 or F_1 is chosen at random for each user, and FID_{EV_i} or FID_{CS_i} are also random in nature. Therefore, it adds the complexity of finding the value of f_i as $o[2^f - 1]$. As a result, it is very tough to transmit false information to $V2G$ communication system users.

F. CONDITIONAL PRIVACY PRESERVATION

In this work, the EV_i or CS_i user hides their actual identity from other system entities using their $\mathbb{S}_{EV_i}$ and OAC. However, CC can find the actual identity of EV_i or CS_i users by using their OAC. For example, if the EV_i or CS_i user is communicating any fake message to the other entities by adding OAC, the CC can verify the content of information with the help of OAC. If communicated information is found as fake, then the CC collects the OAC of the information and identifies the actual identity of EV_i or CS_i users by using their FID_{EV_i} or FID_{CS_i} and tracing table. Next, the CC can expose the privacy of a specific EV_i or CS_i user and it removes the EV_i or CS_i user from the $V2G$ communication system.

G. REPUDIATION ATTACK

In this proposed work, once the EV_i or CS_i user communicates the information to the other entities, they cannot repudiate it because the receiver can check the validity of the EV_i or CS_i user by using the OAC. Similarly, the integrity of information is verified by using the $\mathbb{S}_{EV_i}$ or $\mathbb{S}_{CS_i}$. In case of any dispute, the receiver will verify the information with the help of CC. The CC can identify the actual identity of EV_i or CS_i users with the help of VI_{EV_i} or VI_{CS_i}, which is derived from the received information. After that, CC can reveal the privacy of EV_i or CS_i users and it removes the EV_i or CS_i user from the $V2G$ communication system.

H. UNLINKABILITY DURING DATA COMMUNICATION

In this proposed work, the one-time anonymous signature $\mathbb{S}_{EV_i} = g_2^{1/r_i+EV_{pr_i}+h}$ and the one-time anonymous authentication certificate $OAC = \{\mathcal{M}_1 \parallel \mathcal{M}_2 \parallel FID_{EV_i} \parallel OTC \parallel TI_i$ are self-generated by the EV_i or CS_i user, based on one-time private keys. These one-time private keys will get changed periodically. Therefore, the EV_i or CS_i user will generate a new anonymous signature and certificate for each data communication. Hence, it is not easy for a receiver to identify whether the same user directed the data except for the CC.

I. FORMAL SECURITY VERIFICATION

To validate the security of our proposed approach, we employed the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, aiming to ensure the robustness of the $V2G$ communication system [27]. In the implementation of our suggested scheme, there are three pivotal roles and two composition roles. The basic roles encompass key system entities: the Control Center (CC), Charging Station (CS), and Electric Vehicle (EV). Additionally, the composition roles, namely session and goal & environment roles, serve as indispensable components, capturing various scenarios involving the basic roles.

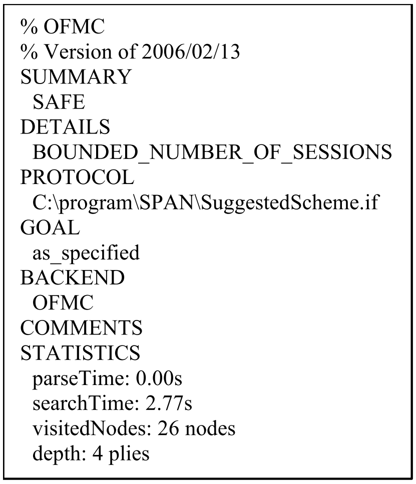
The proposed algorithm undergoes formal security verification through the utilization of the "SPAN (Security Protocol ANimator for AVISPA)" tool. Subsequently, simulation results are obtained by leveraging the OFMC backend, as illustrated in Fig 2. This rigorous security analysis ensures the effectiveness and reliability of our approach in fortifying the $V2G$ communication system against potential threats and vulnerabilities.

VI. PERFORMANCE ANALYSIS

In this section, the performance of the proposed approach is evaluated and compared to other existing schemes in terms of computation, communication, and security features.

A. COMPUTATIONAL COMPLEXITY

In this study, the computational complexity is determined by the time required to verify the user's self-generated signature and certificate for authentication. Specifically, the primary cryptographic operations, including pairing operation (T_p), hash operation (T_h), point multiplication (T_m), and exponential operation (T_e), serve as focal points for assessing computational complexity. To comprehensively analyze computational overhead, cryptographic operations were simulated on a machine equipped with an Intel Core i5-8265U processor and 8-GB RAM capacity. The simulations were conducted using Cygwin 2.9.0 and gcc version 4.9.2 [19],



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\program\SPAN\SuggestedScheme.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.77s
  visitedNodes: 26 nodes
  depth: 4 plies
```

FIGURE 2. The analysis results for security verification using OFMC.

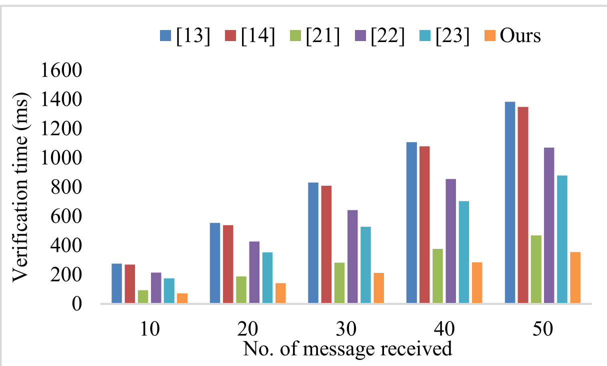


FIGURE 3. Computational complexity of various schemes.

[20]. After simulating cryptographic operations, the time required to execute cryptographic parameters such as T_p, T_h, T_m, T_a, and T_e were calculated as 1.6 ms (milliseconds), 2.7 ms, 3.4 ms, 2.6 ms, and 0.6 ms, respectively. The proposed scheme demonstrates significantly faster cryptographic operations compared to existing schemes, as illustrated in Table 2. Consequently, the proposed scheme completes single cryptographic functions in just 7.10 ms. In contrast, previous schemes [13], [14], [21], [22], [23] require 27.7 ms, 27.0 ms, 9.4 ms, 21.4 ms, and 17.6 ms, respectively, to perform cryptographic operations. The performance analysis depicted in Fig. 3 highlights the minimal time required by the proposed scheme for cryptographic operations, even as the number (n) of users increases.

B. COMMUNICATION COMPLEXITY

The communication complexity of the proposed method is evaluated by considering the size of messages exchanged between EVs and CSs. In this study, the information $rrm_{EV_i} \parallel \mathbb{S}_{EV_i} \parallel s_i \parallel OAC \parallel VI_{EV_i} \parallel TS_i$ is securely communicated from EV_i to CS_i or other EVs. The bit size of TS_i, rrm_{EV_i}, $\mathbb{S}_{EV_i}$, s_i, OAC and VI_{EV_i} is considered as 32$bits$, 160$bits$, 160$bits$, 320$bits$, 160$bits$, and 160$bits$, respectively [24].

TABLE 2. Comparison of computational complexity of various schemes.

Schemes	To verify '1' signature and certificate	To verify 'n' signature and certificate
[13]	$4T_m + T_e + 5T_h \approx 27.7\ ms$	$4nT_m + nT_e + 5nT_h$
[14]	$3T_m + T_e + 6T_h \approx 27.0\ ms$	$3nT_m + nT_e + 6nT_h$
[21]	$2T_m + T_a \approx 9.4\ ms$	$2nT_m + nT_a$
[22]	$4T_m + 3T_a \approx 21.4\ ms$	$4nT_m + 3nT_a$
[23]	$4T_h + 2T_m \approx 17.60\ ms$	$4nT_h + 2nT_m$
Ours	$2T_p + 2T_e + T_h \approx 7.10\ ms$	$(1+n)T_p + 2nT_e + nT_h$

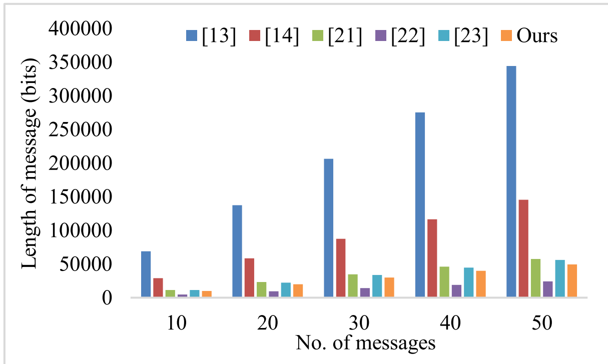


FIGURE 4. Communication complexity of various schemes.

TABLE 3. Communication complexity of various schemes.

Schemes	For single message (bits)	For 'n' messages (bits)
[13]	6880	$6880n$
[14]	2912	$2912n$
[21]	1152	$1152n$
[22]	480	$480n$
[23]	1120	$1120n$
Ours	992	$992n$

The proposed scheme requires a total of 992$bits$(32 + 160 + 160 + 320 + 160 + 160) to communicate a single piece of information. In contrast, other existing schemes such as [13], [14], [21], [22], and [23] necessitate 6880$bits$, 2912$bits$, 1152$bits$, 480$bits$, and 1120$bits$, respectively. The communication complexity of various schemes is summarized in Table 3. As illustrated in Fig. 4, it is evident that the proposed work exhibits lower communication complexity even as the number of messages increases.

TABLE 4. Comparison of security features of various schemes.

Security features	[13]	[14]	[21]	[22]	[23]	Ours
Mutual authentication	✓	✓	✓	✓	✓	✓
Replay attack	×	✓	✓	×	✓	✓
Data integrity	✓	✓	✓	✓	✓	✓
Conditional privacy	×	×	×	×	×	✓
User privacy	✓	✓	✓	✓	✓	✓
Non-repudiation	×	×	×	×	×	✓
Unlinkability	×	×	×	×	×	✓

C. SECURITY FEATURES COMPARISON

The proposed work incorporates a wide range of security features, including mutual authentication, protection against replay attacks, data integrity, conditional privacy, user privacy, and non-repudiation. Table 4 presents a comparative analysis of these security features between the proposed work and other existing schemes. In the table, the symbol '✓' denotes that the system meets the specified security features, while '×' indicates that the scheme lacks provision for the corresponding security features.

Upon examination, it becomes evident that existing schemes [14], [21], and [23] fall short in supporting conditional privacy, non-repudiation, and unlinkability. Furthermore, schemes [13] and [22] neglect to address replay attacks, conditional privacy, non-repudiation, and unlinkability. In contrast, the proposed work stands out by offering comprehensive support for all necessary security features, ensuring robust protection against potential threats and vulnerabilities.

VII. CONCLUSION

This paper presents an efficient mutual and batch authentication system with conditional privacy preservation to ensure secure communication within *IoT* based *V2G* communication system. The proposed scheme enables *EVs* and *CSs* to authenticate each other with minimal computation and communication overhead, addressing a fundamental requirement of *IoT*-based *V2G* systems. By incorporating conditional privacy and implementing a tracing mechanism to identify malicious users, the proposed scheme enhances the efficiency and security of the *V2G* communication system. Furthermore, the introduction of an efficient batch authentication method allows for the validation of multiple *EVs* with reduced computational complexity compared to existing schemes. Through rigorous security and performance analyses, it has been demonstrated that the proposed approach fulfills all essential security requirements while maintaining lower computational and communication overheads. Thus, it is well-suited for resource constrained *V2G* communication systems.

Future Research Direction: Exploring the integration of radio fingerprinting techniques, such as semi-supervised RF fingerprinting with consistency-based regularization and geometric-based channel modelling and analysis for double-RIS aided vehicle-to-vehicle communication systems, with our proposed method presents an exciting avenue for future inquiry. This integration has the potential to enhance the security and reliability of *V2G* communication systems, addressing concerns related to unauthorized access and spoofing attacks. Investigating this fusion could inspire further innovations in the field, leading to the development of more efficient and secure *V2G* communication protocols.

REFERENCES

[1] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2629–2640, Jun. 2018.

[2] B. Kellerhals. (2018). *The Internet of Things Impact on the Smart Grid—Why Security is a Must*. Kyrio. Accessed: Dec. 2019. [Online]. Available: https://www.kyrio.com/blog/internet-ofthings-

[3] K. Kaur, S. Garg, N. Kumar, and A. Y. Zomaya, "A game of incentives: An efficient demand response mechanism using fleet of electric vehicles," in *Proc. 1st Int. Workshop Future Ind. Commun. Netw.*, New Delhi, India, Oct. 2018, pp. 27–32.

[4] X. Hu, K. Wang, X. Liu, Y. Sun, P. Li, and S. Guo, "Energy management for EV charging in software-defined green vehicle-to-grid network," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 156–163, May 2018.

[5] 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.

[6] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

[7] F. Khan, R. L. Kumar, S. Kadry, Y. Nam, and M. N. Meqdad, "Autonomous vehicles: A study of implementation and security," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 11, no. 4, pp. 3013–3021, Aug. 2021.

[8] F. Khan, R. L. Kumar, S. Kadry, Y. Nam, and M. N. Meqdad, "Cyber physical systems: A smart city perspective," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 4, pp. 3609–3616, Aug. 2021.

[9] H. Nicanfar and V. C. M. Leung, "Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 253–264, Mar. 2013.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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, doi: 10.1109/TSG.2016.2602282.

[15] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure V2G networks in the smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 208–220, Feb. 2014.

[16] 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.

[17] K.-S. Kong, W. Lee, Y.-H. Han, and M.-K. Shin, "Handover latency analysis of a network-based localized mobility management protocol," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 5838–5843.

[18] S. Jegadeesan, M. S. Obaidat, P. Vijayakumar, and M. Azees, "SEAT: Secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 815–824, Jun. 2022.

[19] B. Lynn. (2007). *PBC Library—The Pairing-Based Cryptography Library*. Version 0.5. [Online]. Available: http://crypto.stanford.edu/pbc/

[20] (2019). *Cygwin*. [Online]. Available: https://www.cygwin.com/

[21] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1278–1291, Feb. 2021, doi: 10.1109/TVT.2021.3050399.

[22] X. Yang, S. Li, L. Yang, X. Du, and C. Wang, "Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for VANETs," *IEEE Trans. Intell. Transp. Syst.*, early access, 2024, doi: 10.1109/TITS.2024.3367925.

[23] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, S. H. Ahmed, and M. Guizani, "A secure, lightweight, and privacy-preserving authentication scheme for V2G connections in smart grid," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 541–546.

[24] J. Subramani, A. Maria, R. B. Neelakandan, and A. S. Rajasekaran, "Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification," *IET Commun.*, vol. 15, no. 9, pp. 1187–1197, Jun. 2021.

[25] S. Jegadeesan, M. S. Obaidat, P. Vijayakumar, M. Azees, and M. Karuppiah, "Efficient privacy-preserving anonymous authentication scheme for human predictive online education system," *Cluster Comput.*, vol. 25, no. 4, pp. 2557–2571, Aug. 2022.

[26] X. Zeng, G. Xu, X. Zheng, Y. Xiang, and W. Zhou, "E-AUA: An efficient anonymous user authentication protocol for mobile IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1506–1519, Apr. 2019.

[27] S. Jegadeesan, M. Azees, N. R. Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020.

JEGADEESAN SUBRAMANI received the B.E. degree from Periyar University, the M.E. degree from the Anna University of Technology, and the Ph.D. degree from Anna University. He is currently a Professor with the M. Kumarasamy Engineering College. He has published extensively in prestigious journals, such as IEEE TRANSACTIONS, *IEEE Magazine*, IEEE ACCESS, Elsevier, Springer, IET, and Wiley, contributing significantly to the advancement of his field. His research interests include wireless sensor networks, fog computing, blockchain, smart grids, vehicle ad hoc networks, and wireless body area networks. He is a Registered Patent Agent.

AZEES MARIA (Member, IEEE) received the B.E. degree in electronics and communication engineering and the M.E. degree in applied electronics from the St. Xavier's Catholic College of Engineering, Nagercoil, India, which is affiliated under Anna University, Chennai, India, in 2011 and 2013, respectively, and the Ph.D. degree from the Faculty of Information and Communication Engineering, Anna University, in 2017. He is currently an Assistant Professor with VIT-AP University, India. He has published research articles in some of the reputed journals, such as the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Cluster Computing* (Springer), and *IET Intelligent Transport Systems*. His research interests include security in wireless sensor networks, blockchain technology, fog computing, and VANETs. He is also one of the Academic Editor of *Security and Communication Networks* (Wiley).

ARUN SEKAR RAJASEKARAN (Member, IEEE) received the bachelor's degree in electronics and communication engineering from the Sri Ramakrishna Engineering College, in 2008, and the master's degree in VLSI design and the Ph.D. degree in low-power VLSI design from Anna University, Chennai, in 2013 and 2019, respectively. He is currently an Associate Professor with the Department of Electronics and Communication Engineering, SR University, Warangal, Telangana, India. He has nearly 14 years of teaching experience. He had published more than 27 papers in international conferences and 25 reputed indexed journals namely, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Springer, *Microprocessor and Microsystems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *IET Communications*, IEEE ACCESS, and *Concurrency and Computation* (Wiley). His research interests include low-power VLSI design, network security, blockchain, body area networks, and image processing. He is a Life Member of ISTE, IETE, ISRD, and IEANG.

BABJI PRASAD CHAPA received the B.Tech. degree in electronics and communication engineering and the M.Tech. degree in systems and signal processing from JNT University, Hyderabad, in 2007 and 2010, respectively, and the Ph.D. degree from Andhra University, in 2020. He has a teaching experience of 15 years. He was a project guide for several UG and PG students. He has published more than 30 articles in journals and around 20 papers in national/international conferences. His research interests include wireless communications and cognitive radio networks. He was a recipient of the Best Teacher Award.