Computer Networks 217 (2022) 109335

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

An energy-efficient and secure identity based RFID authentication scheme for vehicular cloud computing

Waseem Akram [a], Khalid Mahmood [b,c], Xiong Li [d], Mazhar Sadiq [e], Zhihan Lv [f], Shehzad Ashraf Chaudhry [g,h,*]

[a] Department of Computer Science, Lahore Garrison University, Main Campus, Lahore, Pakistan
[b] Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin, 64002, Taiwan, ROC
[c] Department of Mathematics, University of Padua, 35131 Padua, Italy
[d] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
[e] Department of Computer Science, COMSATS University, Islamabad, Sahiwal Campus, Pakistan
[f] Department of Game design, Faculty of Arts, Uppsala University, Uppsala, Sweden
[g] Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates
[h] Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul, Turkey

ARTICLE INFO

Keywords:
Authentication
Mutual authentication
Identity based authentication
Vehicular cloud computing

ABSTRACT

Vehicular Cloud Computing (VCC) is a contemporary paradigm that includes the Internet of Things (IoT), cloud computing, and vehicular networking technologies. VCC offers vehicle-to-device, vehicle-to-infrastructure, and vehicle-to-vehicle communication in which the vehicles can communicate using sensing abilities. VCC is exploiting the IoT environment, cloud architecture, and vehicle resources. However, the energy-efficient privacy of communicators and security of communication are assertive problems in VCC. To accomplish this goal, we present an identity-based authentication scheme for VCC which also uses radio frequency identification (RFID). The security and robustness of the devised scheme are evaluated using informal and formal analysis. The informal analysis shows that our scheme is vigorous to resist various attacks. The formal analysis is done through Random Oracle Model (ROM) which shows that the scheme is secure and efficient. The performance of our scheme is also determined and compared with various related schemes which clearly illustrate the efficiency of the proposed scheme. Thus, our scheme is very efficient for employment in the VCC environment.

1. Introduction

The advancements in software, hardware, and communication architectures are empowering the implementation and study of different network applications used in numerous architectures. In the current decade, the vehicular ad-Hoc network (VANET) [1–3] and vehicular cloud computing (VCC) has got much attention. In an ordinary network of vehicles, VANET and VCC are evolved as novel archetypes for exchanging information. In vehicular communication, VCC offers various advantages of cloud infrastructure to use electronic resources for communications of vehicles. The actual goal of VCC is to provide numerous facilities of computations to vehicles in real-time which are equipped with low computing devices to optimize traffic congestion, travel time and avoid accidents. Thus, the adoption of VCC technology will be environmentally friendly. Furthermore, VCC provides technically sound incorporation of intelligent transportation, wireless sensor networks and mobile cloud computing for ensuring a perceptive environment of urban transport and to achieve road safety [4,5].

In VCC, every vehicle is linked with another vehicle or connected with the infrastructures through the vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communication network [6]. VCC utilizes various utilities of the cloud such as platform, Infrastructure, Computing, Storage, Network, Entertainment, and Data. The platform as a utility can be followed as it provides the domain of VCC communication. This application may consist of various utilization like details about roadside units, base stations, managing staff availability, accumulating traffic information, maintaining the skillful, intelligent environment, and sending message alerts in case of urgency using the response from the clients depending on their preceding information. In this architecture, the cloud contributes to get, process and maintain the relevant data of the user. The cloud is supposed to be synchronized with

* Corresponding author.
E-mail address: ashraf.shehzad.ch@gmail.com (S.A. Chaudhry).

https://doi.org/10.1016/j.comnet.2022.109335
Received 8 November 2021; Received in revised form 20 July 2022; Accepted 27 August 2022
Available online 3 September 2022

all the base stations on the roadside unit, where the real-life security problems of clients may appear [7,8].

RFID is a well-known technology that deals with the unique recognition of objects. This technology was used to differentiate and detect the weapons of friends and enemies. This technology thriving speedily due to its numerous applications till now. There are various applications of RFID such as billing and tracking process, toll collection and contactless payment, airport baggage tracking logistics, tracking of goods, access management, machine-readable travel documents, and many more [9–11]. Currently, the healthcare system, baggage identification at airports, management system, and passport identification are such areas where RFID is used. The contact-less recognition of objects eradicates the conventional bar-code infrastructure. The vehicles are equipped with a low-frequency reader to retrieve the client's information within a recommended area of communication networks.

RFID reader offers assistance in situations of accidents, damage, unavailability, and urgency in vehicles. RFID also maintains higher error tolerance in networks of communication. Ultra-high frequency is used by the readers deployed on the roadside unit in vehicles. Radio waves are used in the network shared between the reader and tag with numerous frequencies such as IEEE 802.15.4 Zigbee. RFID based technology provides the assistance for user about vehicles [12–15]. In VANET, vehicles are equipped with RFID-based devices which help to gather the information of the user. As the number of vehicles is rising, there is a requirement for more dedicated resources and adequate utilities for vehicle users. Thus, developing an efficient, secure, and robust RFID-based authentication scheme is a prudent idea for VCC. Recently, various researchers proposed numerous authentication and anonymous schemes for VCC. However, the RFID-based schemes for VCC are not focused. In these types of systems, the RFID tag must be registered as anonymous. To maintain the privacy of the reader and tag, un-traceability and anonymity are required. In this article, we develop an anonymous identity-based mutual authentication scheme using RFID technology for the VCC environment.

2. Related work

Mutual authentication and privacy-preserving schemes are developed for ensuring privacy, authentication, and security problems in the RFID-enabled VCC environment. Ahamed et al. [16] presented elliptic curve cryptography (ECC) based key agreement scheme using RFID in order to deal with the security problems such as physical attacks, eavesdropping, and tracking. Ahamed et al. [17] also proposed a second authenticated key agreement scheme that utilized the approach of server-less authentication. Tian et al. [18] suggested an authentication scheme using RFID. They declared that the security properties are used to investigate the security of the framework. However, Lv et al. [19] analyzed and reveal that the scheme in [18] is inefficient to resist information leakage attacks. Chen et al. [20] devised an RFID-based key agreement scheme and claim that it resists replay attack and backward secrecy.

Liao et al. [21] suggested an ECC-based key agreement scheme and claimed that their scheme resists eavesdropping, replay, and denial of service attacks. However, Peeters et al. [22] showed that the scheme in [21] is not efficient and also vulnerable to various security attacks such as server spoofing, tag cloning, and tag impersonation attack. Chou [23] suggested an ECC-based privacy-preserving authentication scheme using RFID and declared that their scheme is efficient to resist masquerading, perfect forward secrecy, and replay attacks. However, Farash [24] analyzed and declared that their scheme fails to resist masquerading, replay attack and also does not offer mutual authentication. Srivastava et al. [13] proposed a hash-based authentication scheme for cloud environment. Later on, Li et al. [14] analyzed and found that the scheme [13] presented insecure authentication phase. Further, Li et al. presented an enhanced scheme for secure cloud communication. Naeem et al. [25] also presented an authentication scheme for RFID system. However, Izza et al. [26] found some weaknesses in their scheme including lack of anonymity and authentication.

Yan et al. [27] presented an authenticated key agreement scheme for vehicular cloud computing. Their scheme offers efficient privacy and security to vehicular infrastructure. It was the first article that emanates the issues of security in VCC. Tsai and Lo [28] presented a privacy-preserving and secure key agreement scheme for cloud computing. They declared that their devised scheme is efficient, secure, and offers mutual authentication between client and server. He et al. [29] noticed the security problems in the scheme of Tsai and Lo [28] and declared that their scheme fails to resist masquerading attacks. Afterward, He et al. devised an enhanced authentication scheme on mobile cloud computing. Wang et al. [30] introduced a lightweight authenticated key agreement scheme.

Liu et al. [31] introduced an authentication scheme for the internet of vehicles and declared that the devised scheme is convenient and robust for the vehicle to vehicle communication. It also improved the security of vehicular network communication. Jiang et al. [32] devised an identity-based authentication scheme for vehicular cloud computing. Shi et al. [33] proposed an ECC-based user authentication scheme for wireless sensor networks (WSNs) which is inefficient to resist insider, offline password guessing attacks and also violates anonymity. Choi et al. [34] presented an ECC-based user authentication scheme that is vulnerable to impersonation attacks and also fails to offer reliable mutual authentication and password modification phase. Yu et al. [35] proposed an efficient authentication scheme for WSNs in vehicular communication which is inadequate to provide mutual authentication and vulnerable to masquerading and session key security attack. Liu et al. [36] suggested a temporal credential-based key agreement scheme for the applications of WSN such as safety checking in coal mines. However, their scheme [36] fails to resist offline password guessing, session key leakage, impersonation, and desynchronization attack. Kumari and OM [37] presented an authentication scheme for the various applications of WSN which is susceptible to insider, masquerading and offline password guessing attacks. Vijayakumar et al. [38] proposed an authenticated key agreement scheme for vehicular ad-hoc communications.

In authenticated key agreement schemes, asymmetric cryptographic techniques have been widely used. Currently, many asymmetric cryptographic techniques can be used to develop authentication and key agreement schemes i.e., ECC, bilinear pairing, RSA, and so on. Prominently, another technique i.e., chaotic maps (e.g., Chebyshev-maps, Logistic maps) has been generally noticed by various researchers [39]. Chaotic maps refer to arbitrary movement in the deterministic system, whose demeanor is unpredictable, unrepeatable, and uncertain. Exclusively, in cryptography, chaotic maps have been broadly utilized in order to develop authentication schemes. For the first time, Xiao et al. [40] proposed an authenticated key agreement scheme by utilizing chaotic-maps for an E-commerce environment. Later, Alvarez [41] claimed that the scheme of Xiao et al. [40] has various limitations of efficiency, security, and inefficient to resist counterfeiting attacks. Moreover, Xiao et al. [42] enhanced the scheme [40] and proposed chaotic maps based untraditional key agreement scheme. Since then, a huge number of key agreement schemes [43–57] have been presented for various scenarios of applications.

Numerous authentication schemes have been presented for VCC. Unfortunately, most of these schemes are vulnerable to some major attacks or have some other security-related issues. Moreover, authentication schemes for the RFID-based VCC environment are missing. So, in this article, our focus is to develop an authentication scheme for VCC that employs the RFID.

2.1. Motivation and contributions

It is obvious from the recent literature that multiple authentication protocols have been designed for vehicular cloud computing (VCC).

Table 1
Common used notations.

Common Notations	Elucidation
$\mathcal{T}_i$	ith Tag
id_i	Identity of $\mathcal{T}_i$
PID_i	Pseudo Identity of $\mathcal{T}_i$
$\mathcal{R}_j$	jth Reader
id_j	Identity of $\mathcal{R}_j$
CDS_s	Cloud Data Server
PID_s	Pseudo Identity of CDS_s
sr	Master Key of System
$\mathcal{E}_{adv}$	The Adversary
$sig(.)$	Signature
$Ver(.)$	Verification of signature
$\Rightarrow$	Private Communication Channel
$\rightarrow$	Public Communication Channel
$T_s(x)$	Chebyshev Chaotic Map Operation

However, the authentication protocols for RFID-enabled VCC are not appropriately designed. Since the VCC and RFID have their own privacy requirements and computing abilities; therefore, it has become an essential need to design an authentication protocol for RFID-enabled VCC systems. In this article, we propose an authentication protocol for the RFID-enabled VCC system using Chebyshev Chaotic map operation. The key contributions of our proposed protocol are discussed in subsequent points:

- The authentication process of the proposed protocol supports the establishment of a session key between the cloud data server and RFID tag.
- The proposed RFID-enabled authentication protocol is evaluated informally and formally to evaluate its security strength. The informal security evaluation is conducted using the assumptions of the threat model, while the formal security evaluation of the proposed protocol is carried out using the widely used random oracle model.
- The security evaluation of the proposed protocol proves its security strength against well-known security threats.
- The performance of the proposed protocol is evaluated and compared with recent related protocols. The performance evaluation shows the supremacy of the proposed protocol in terms of computation, communication cost, and security features as compared to related protocols.

2.2. Outline

The rest of the article is organized as follows: Section 3 presents the preliminaries which are used in designing the protocol. The details of the proposed protocol are presented in 4. Section 5 solicits the security evaluation, while Section 6 presents the performance analysis. At last, the conclusion is presented in Section 7.

3. Preliminaries

In this section, we discuss the preliminaries that are used in the design of our protocol including threat model, chaotic map, and notation guide that is given in Table 1.

3.1. Threat model

This section presents the attacker capabilities under the common adversarial model as adopted in numerous studies [58–64]:

- An adversary $\mathcal{E}_{adv}$ may wish to disrupt communication between readers, RFID-assisted tags, or the cloud data server over a public channel.
- To deal with the tag and the reader, $\mathcal{E}_{adv}$ can use an active attack, a passive attack, or a combination of both.
- $\mathcal{E}_{adv}$ can use rouge readers or tags in the formations to impersonate as the appropriate readers and tags while applying aggression.

3.2. Chaotic map

Definition 1. Suppose $num \in Z^*$ and $y \in \{-1, 1\}$ are real numbers, $T_n(y) : \{-1, 1\} \rightarrow \{-1, 1\}$ express Chebyshev polynomial and is written as $T_{num}(y) = cos(num.cos^{-1}(y))$, while the recurrence relationship is shown as $T_{num}(y) = 2yT_{num-1}(y) - T_{num-2}(y)$, where $num \geq 2$, $T_0(y) = 1$ and $T_1(y) = y$.

Proposition 1. *The semigroup property closes the Chebyshev polynomial, which means:* $T_m(T_n(y)) = cos(r.cos^{-1}(cos(s.cos^{-1}(y))))$ $= cos(mn.cos^{-1}(y)) = T_{nm}(y), where, m \in Z^*$ *and* $y \in \{-1, 1\}$.

Definition 2 (*CMDLP*)**.** In the case of a given real number $y \in \{-\infty, +\infty\}$ and an extended Chebyshev polynomial x, according to the Chaotic-maps discrete logarithm problem, it is difficult for an adversary. $\mathcal{E}_{adv}$ to calculate m (the secret integer) so that $x = T_m(y) mod\ q$. That is, for any $\mathcal{E}_{adv}$ within a bounded time t_{bt}, the probability $Advnt_{\mathcal{E}_{adv}}^{CMDLP} t_{bt} Pr[\mathcal{E}_{adv}(x, y) = m : m \in Z_q^*, x = T_m(y) mod\ q]$ is negligible, i.e. $Advnt_{\mathcal{E}_{adv}}^{CMDLP} t_{bt} \leq \varepsilon$, where ε refers to some negligible function.

Definition 3 (*CMCDHP*)**.** In the case of a given real number $y \in \{-\infty, +\infty\}$ and two extended Chebyshev polynomials $T_m(y) mod q$ and $T_n(y) mod q$, the Chaotic-maps computational Diffie–Hellman problem states that it is difficult for an $\mathcal{E}_{adv}$ to calculate $T_{nm}(y) mod q$. That is, for any $\mathcal{E}_{adv}$ within a bounded time t_{bt}, the probability $Advnt_{\mathcal{E}_{adv}}^{CMCDHP} t_{bt} = Pr[\mathcal{E}_{adv}(y, T_n(y) mod\ q,\ T_m(y) mod\ q) = T_{nm}(y) mod\ q : n, m \in Z_q^*]$ is negligible, i.e. $Advnt_{\mathcal{E}_{adv}}^{CMCDHP} t_{bt} \leq \varepsilon$, where ε refers to some negligible function

3.3. Network model

The generic architecture diagram of RFID-enabled VCC is illustrated in Fig. 1. This architecture mainly comprises three participants: vehicles, Road-Side Units (RSUs), and Cloud Data Server (CDS). The vehicles are equipped with RFID tags whereas, RSUs are furnished with high-frequency RFID readers. The tags on vehicles allow RSU to collect its information (e.g., traffic information, road condition, alerts in case of emergency, etc.) through an RFID reader. Such information is then relayed to CDS for storage and further analysis. The results of this analysis can be helpful to draw some concrete solutions. For instance, it can help to predict road accidents in a particular region. In the whole scenario, the communication channel is public. Thus, there is a dire need to implement an efficient and reliable mechanism to securely transmit the information. Therefore, several researchers have contributed to designing mutual authentication protocols for the RFID-based VCC ecosystem.

4. Proposed protocol

The designed chaotic map-based authentication protocol for RFID-enabled vehicular cloud computing is briefly described in this section. In the presented protocol, the cloud database server CDS_s and tag $\mathcal{T}_i$ communicate with each other through the tag reader $\mathcal{R}_j$ in order to exchange shared key SK. The phases of our protocol are briefly explained in the trailing subsections.

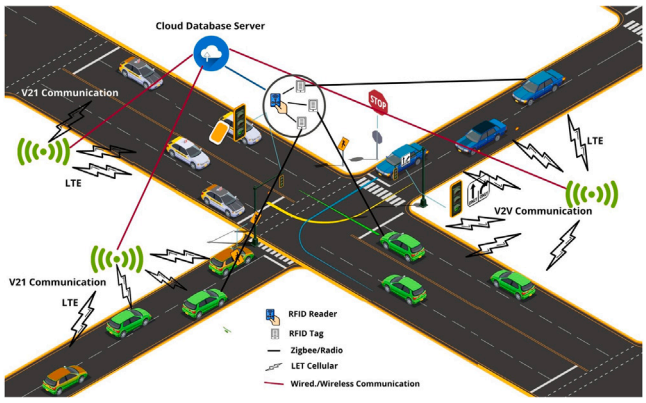

Fig. 1. Network model of vehicular cloud computing.

4.1. Tag registration

This phase portrays the registration process performed between $\mathcal{T}_i$ and CDS_s. Each $\mathcal{T}_i$ must get registered with CDS_s to become the legal entity of the system. The registration phase as illustrated in Figs. 2 and 3 is summarized as follows:

1: Firstly, $\mathcal{T}_i$ picks unique id_i and produces n_1. Thereafter, $\mathcal{T}_i$ computes:

$$A_i = sig(id_i \| Rev_i \| n_1) \tag{1}$$

Next, $\mathcal{T}_i$ sends $\{id_i, A_i, n_1\}$ towards CDS_s along with registration request.

2: CDS_s receives $\{id_i, A_i, n_1\}$ and sets revocation value $Rev_i = 0$. Next, CDS_s checks whether $Ver(A_i, id_i \| Rev_i \| n_1) \stackrel{?}{=} 1$. If it returns true, CDS_s perceives that $\mathcal{T}_i$ has not already revoked. Therefore, CDS_s generates: n_2 and computes:

$$\omega_s = h(sr||PID_s), T_{\omega_s}(x) \tag{2}$$

$$X_i = h(id_i||\omega_s) \tag{3}$$

$$PID_i = E_{T_{\omega_s}}(id_i \| n_2 \| \omega_s) \tag{4}$$

Finally, CDS_s sends registration parameters $\{PID_i, X_i\}$ toward $\mathcal{T}_i$.

3: Upon receiving $\{PID_i, X_i\}$ from CDS_s, $\mathcal{T}_i$ computes: $\prec_i = id_i \oplus X_i$ and keeps $\{PID_i, \prec_i\}$ in its memory.

4.2. Authentication phase

The authentication phase of presented protocol is explained in this subsection. The step-by-step procedure of this phase as shown in Figs. 4 and 5 is described as follows:

1: Initially, $\mathcal{T}_i$ inserts id_i and generates: n_3. Next, $\mathcal{T}_i$ computes

$$X_i = \prec_i \oplus id_i \tag{5}$$

$$M_1 = T_{n_3}(x) \ mod \ P \tag{6}$$

$$M_2 = h(id_i \| M_1 \| X_i) \tag{7}$$

Thereafter, $\mathcal{T}_i$ sends $\{PID_i, M_1, M_2\}$ as login request towards $\mathcal{R}_j$.

2: Whenever, $\mathcal{R}_j$ receives the message from $\mathcal{T}_i$, it add its identity id_j and relays the message $\{PID_i, M_1, M_2, id_j\}$ to CDS_s.

3: On getting $\{PID_i, M_1, M_2, id_j\}$ from $\mathcal{R}_j$, CDS_s computes:

$$(id_i \| n_2 \| \omega_s) = D_{T_{\omega_s}}(PID_i) \tag{8}$$

$$X_i = h(id_i||\omega_s) \tag{9}$$

Later, it verifiers: $M_2 \stackrel{?}{=} h(id_i \| M_1 \| X_i)$. In case of successful verification, CDS_s generates random numbers n_4 and computes: $PID_i^{i+1} = E_{T_{\omega_s}}(id_i \| n_4 \| \omega_s)$, $M_3 = T_{n_4}(x) \ mod \ P$, $SK = T_{n_4}(M_1) \ mod \ P$, $M_4 = h(id_i \| PID_s) \oplus (M_3 \| PID_i^{i+1})$ and $M_5 = h(id_i \| PID_s \| SK \| M_3 \| X_i)$. At the end, CDS_s conveys the message $\{M_4, M_5\}$ towards $\mathcal{R}_j$.

4: $\mathcal{R}_j$ receives the message from CDS_s and relays $\{M_4, M_5, id_j\}$ toward $\mathcal{T}_i$.

5: Whenever $\mathcal{T}_i$ gets $\{M_4, M_5, id_j\}$ from $\mathcal{R}_j$, it computes:

$$(M_3 \| PID_i^{i+1}) = h(id_i \| PID_s) \oplus M_4 \tag{10}$$

$$\acute{SK} = T_{n_3}(M_3) \ mod \ P \tag{11}$$

Finally, $\mathcal{T}_i$ authenticates $M_5 \stackrel{?}{=} h(id_i \| PID_s \| \acute{SK} \| M_3 \| \acute{X}_i)$. If successful, both $\mathcal{T}_i$ and CDS_s agree on common session key SK for secure communication.

5. Security evaluation

This section highlights the security evaluation of the proposed protocol using informal and formal security evaluation. The details are described in subsequent subsections.

5.1. Informal security evaluation

This section solicits the informal security evaluation of our protocol. For such evaluation, we have followed the threat model as presented in Section 3.1.

5.1.1. Tag anonymity and untraceability

In our protocol, $\mathcal{T}_i$ does not exchange its identity id_i over public channel. In addition, there is no hint of id_i for adversary $\mathcal{E}_{adv}$ in the public message $\{PID_i, M_1, M_2\}$ sent by $\mathcal{T}_i$. Moreover, the unique pseudo identity PID_i is utilized for each session so that $\mathcal{E}_{adv}$ can never trace $\mathcal{T}_i$ by monitoring two distinct messages of same $\mathcal{T}_i$. Since $\mathcal{E}_{adv}$ can neither determine the real id_i of $\mathcal{T}_i$ nor he can track his activities from public channel messages. Hence, it is justified that our protocol preserves anonymity and untraceability properties.

5.1.2. Tag impersonation attack

In order to impersonate $\mathcal{T}_i$, $\mathcal{E}_{adv}$ may try to regenerate the message $\{PID_i, M_1, M_2\}$. Although, $\mathcal{E}_{adv}$ can produce n_3; nevertheless, the generation of such message requires both id_i and X_i. It is worth noticing that it is infeasible for $\mathcal{E}_{adv}$ to access these values since they are not kept anywhere. Consequently, the presented protocol withstands against $\mathcal{T}_i$ impersonation attack.

5.1.3. Cloud database server impersonation attack

In the designed protocol, if $\mathcal{E}_{adv}$ intends to launch impersonation on CDS_s then he has to generate valid $\{M_4, M_5\}$. It can be noticed that $\mathcal{E}_{adv}$ needs to determine id_i first along with the credentials stored inside the database. However, all these tasks require the secret key sr of CDS_s which is solely possessed by CDS_s. Hence, we can justify that our protocol withstands against CDS_s impersonation attack.

5.1.4. Ephemeral secret leakage (ESL) attack

During the execution of designed protocol, both $\mathcal{T}_i$ and CDS_s establish session key as $SK = T_{n_4}(M_1) \ mod \ P = T_{n_3}(M_3) \ mod \ P = \acute{SK}$. Assume that $\mathcal{E}_{adv}$ wants to generate SK from the public messages. However, it is worth noticing that the establishment of SK involves ephemeral secrets n_3 and n_4. These ephemeral secrets are freshly generated for each session and not exchanged over an open channel. Thus, the presented protocol is robust against ESL attacks. Moreover, the involvement of such secrets makes SK of any particular session different from the SK of all forthcoming and previous sessions.

$\mathcal{T}_i$	$\mathcal{CDS}_s$
Registration Phase	
Chooses id_i	
Generates: n_1	
Computes: $A_i = sig(id_i \| Rev_i \| n_1)$	
$\xrightarrow{\{id_i, A_i, n_1\}}$	
	$Ver(A_i, id_i \| Rev_i \| n_1) \stackrel{?}{=} 1$
	Generates: n_2
	Computes:
	$\omega_s = h(sr \| PID_s), T_{\omega_s}(x)$
	$X_i = h(id_i \| \omega_s)$
	$PID_i = E_{T_{\omega_s}}(id_i \| n_2 \| \omega_s)$
$\xleftarrow{\{PID_i, X_i\}}$	
$\prec_i = id_i \oplus X_i$	
Keeps $\{PID_i, \prec_i\}$ in its memory	

Fig. 2. Registration phase.

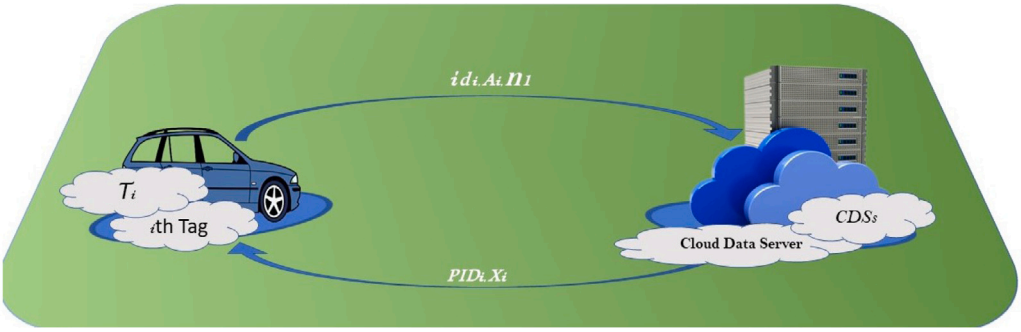

Fig. 3. Registration phase of proposed protocol.

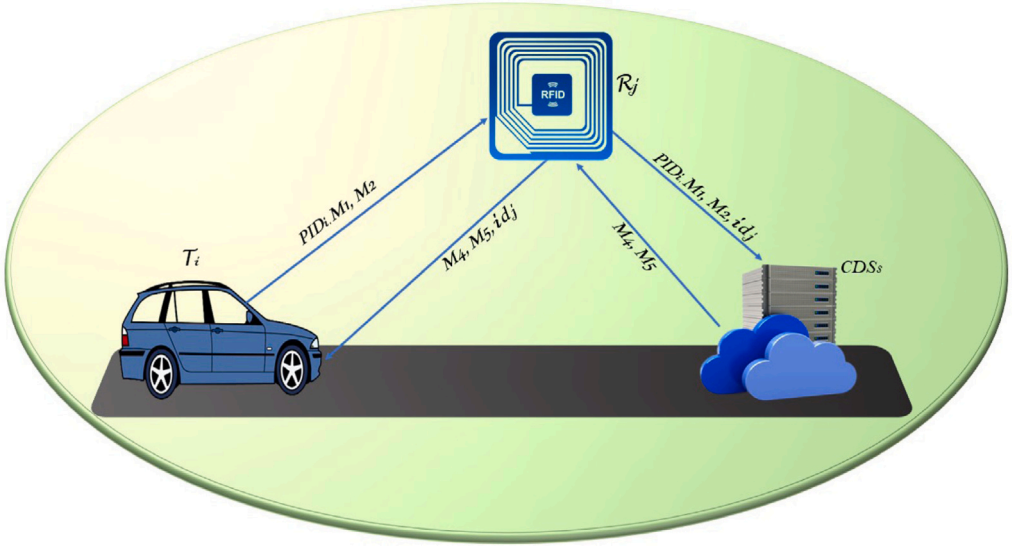

Fig. 4. Authentication phase of proposed protocol.

5.1.5. Man-in-the-Middle (MITH) attack

Assume that an $\mathcal{E}_{adv}$ eavesdrops on the public communicated messages of the designed protocol. In order to convince $\mathcal{T}_i$ and $\mathcal{CDS}_s$, $\mathcal{E}_{adv}$ may try to tamper such messages. However, $\mathcal{E}_{adv}$ needs id_i, X_i and sr to alter these messages which are not available to $\mathcal{E}_{adv}$. Therefore, the presented protocol is resilient against MITH attacks.

5.1.6. Free from synchronization issue

The clock synchronization is needed when timestamps are used in any authentication protocol so that the entities can be synchronized to verify the freshness of received messages. Nevertheless, the proposed protocol is free from clock synchronization issues since we utilize random numbers instead of timestamps to check the freshness of received messages.

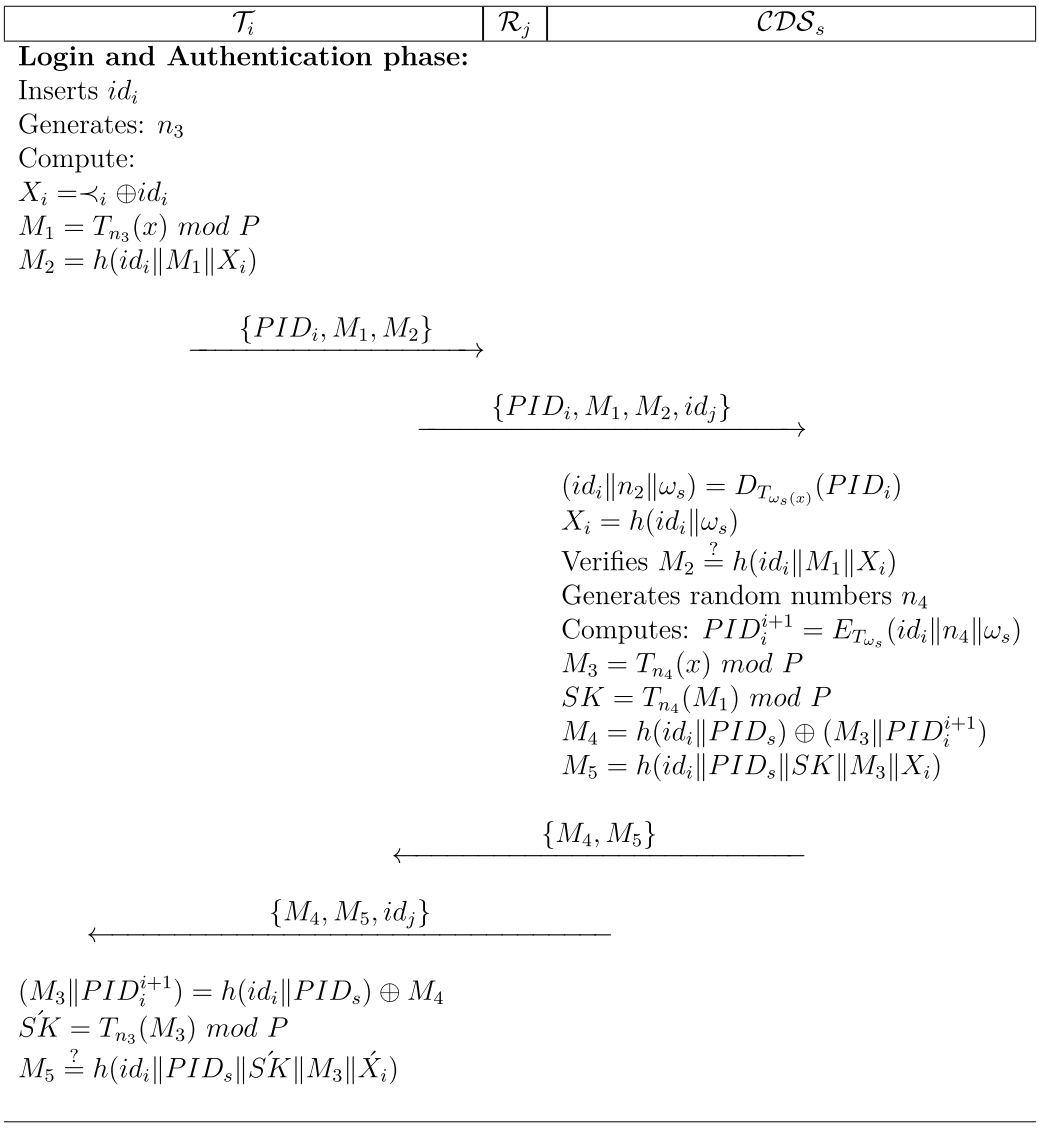

Fig. 5. Login and authentication phase of proposed scheme.

Table 2
Queries and their Description.

Query	Description
$System - setup$	C_{chl} returns parameters to $\mathcal{E}_{adv}$ when this query is executed.
$h(m_y)$	C_{chl} selects arbitrary $r_y \in Z_q^*$, add$\{m_y, r_y\} l_m$ it to the list, and respond r_y to $\mathcal{E}_{adv}$ when this query is executed.
$Send(E\text{th}, M)$	By this query, $\mathcal{E}_{adv}$ sends out M and C_{chl} responses in accordance with the proposed (AKAP) protocol's segregation.
$CorruptT$	When this query with id_i is executed, C_{chl} responds with a secret key to $\mathcal{E}_{adv}$.
$CorruptCSD$	When this query with id_j is executed, C_{chl} responds with a secret parameter PID_i to $\mathcal{E}_{adv}$.
$Reveal(E\text{th})$	By running this query helps to share the session key SK between Eth and $\mathcal{E}_{adv}$.
$Test(E\text{th})$	$\mathcal{T}_A$ request is made to Eth for the session key SK, and Eth responds with the conclusion of a flipped unbiased coin c_{coin}.

5.2. Formal security evaluation

This section solicits the formal security evaluation of our proposed protocol. We examine the generally accepted adversarial model outlined in Section 3.1.

Security Model In this article, we used the security model used in [29,65] to formally demonstrate the robustness of the authentication and key agreement protocol (AKAP) under the RoM model [66]. An $\mathcal{E}_{adv}$ connects implementing entities in the ROM model i.e $\mathcal{T}_i$ and CDS_s. As shown in Table 2, $\mathcal{E}_{adv}$ can run various queries and the challenger C_{chl} responds accordingly.

During query Test, $\mathcal{E}_{adv}$ can assume the value of a flipped coin c_{coin}. If $c_{coin} = c_{coin}$, $\mathcal{E}_{adv}$ compromises the security of the introduced protocol ϵ. Now, let the event begin. The event E_{evt} is the correct prediction of coin c_{coin}. The benefits of $\mathcal{E}_{adv}$ is denoted by the symbol $Advnt_{\mathcal{E}_{adv}}^{AKAP}$. Here are some definitions:

Definition 4. ($AKAP_{CDS_s}^{T_i}$): The proposed AKAP protocol ϵ is $AKAP_{CDS_s}^{T_i}$-Secure if $Advnt_{\mathcal{E}_{adv}}^{AKAP}$ is negligible. The proposed AKAP protocol offers mutual authentication ($M_u A_t$) between $\mathcal{T}_i$ and a CDS_s via $\mathcal{R}_j$ arbitration if $\mathcal{E}_{adv}$ cannot create any of the: 1 legal login request message by $\mathcal{T}_i$, 2 arbitration message by $\mathcal{R}_j$ and 3 response message by CDS_s. Let E_t, E_R, E_{CDS} shows event that $\mathcal{E}_{adv}$ can provoke message

1,2 and 3 respectively. $\mathcal{E}_{adv}$'s advantage to crack M_uA_t of AKAP can be explained as $Advnt^{M_uA_t}_{AKAP}(\mathcal{E}_{adv}) = Pr[E_t] + Pr[E_R] + Pr[E_{CDS}]$.

Definition 5. ($M_uA_t{}^{T_i}_{CDS_s}$): The proposed AKAP protocol ϵ is $M_uA_t{}^{T_i}_{CDS_s}$ Secure if $Advnt^{MA}_{AKAP}\mathcal{E}_{adv}$ is negligible.

Provable Security: This section demonstrates the security of the proposed AKAP protocol using the security model defined in the preceding section.

Theorem 1. *Mutual authentication is achieved using the proposed AKAP protocol.*

Proof. An adversary $\mathcal{E}_{adv}$ may consider running the query Send($\mathcal{T}_i$, M_1) and seeing if the challenger C_{chl} receives verification $M_2 \stackrel{?}{=} h(id_i\|M_1\|X_i)$, then M_1 is legal, where $M_1 = \{PID_i, M_1, M_2\}$. C_{chl} can validate the legitimacy and freshness of M_1 using master key sr. C_{chl} has the probability $\frac{1}{p_h}$ of obtaining a record from the maintained list l_m. As a result, $\mathcal{E}_{adv}$ can create M_1, and the probability of this happening is $Pr[E_t] = \frac{1}{p_h}$. An adversary $\mathcal{E}_{adv}$ may consider running the query Send($\mathcal{R}_j, M_2$) and seeing if the challenger C_{chl} receives verification $M_2 \stackrel{?}{=} h(id_i\|M_1\|X_i)$, then M_2 is legal, where $M_2 = \{PID_i, M_1, M_2, id_j\}$. C_{chl} has the probability $\frac{1}{p_h}$ of obtaining a record from the maintained list l_m. If two legitimate messages $\langle PID_i, M_1, M_2, id_j\rangle$ and $\langle \overline{PID_i}, M_1, M_2, id_j\rangle$ are created then C_{chl} can compute $(e_1 - \overline{e_1}).P_{pub}$. As a result, the event probability is $Pr[E_R] = \frac{1}{q.p_h^2}$. At last, $\mathcal{E}_{adv}$ may consider running the query Send(CDS, M_3) and seeing if the challenger C_{chl} receives verification $M_5 \stackrel{?}{=} h(id_i\|PID_s\|\acute{SK}\|M_3\|\acute{X}_i)$, then M_3 is legal, where $M_3 = \{M_4, M_5\}$. If two legitimate messages $\langle M_4, M_5\rangle$ and $\langle \overline{M_4}, \overline{M_5}\rangle$ are created then C_{chl} can compute $(e_1 - \overline{e_1}).P_{pub}$ with the probability $\frac{1}{q}$; furthermore C_{chl} has the probability $\frac{1}{p_h}$ of obtaining a record from the maintained list l_m. As a result, the probability of this event is $Pr[E_{CDS}] = \frac{1}{p_h}$. $\mathcal{E}_{adv}$ has the ability to create M_3, and the probability is $\frac{1}{q.p_h}$. So, we can conclude that $Advnt^{AKAP}_{\mathcal{E}_{adv}}$ is negligible.

Theorem 2. *The proposed AKAP protocol is semantically secure if DLP over IBC is hard.*

Proof. When querying Test, C_{chl} has a non-negligible advantage λ in obtaining the correct session key (SK); this event is represented by E_{SK}. The probability of $\mathcal{E}_{adv}$ guessing c_{coin} during the Test session is $\geq \frac{1}{2}$, as a result, $Pr[E_{SK} \geq \frac{\lambda}{2}]$. Let E^T_{Tst} and E^{CDS}_{Tst} shows the event that $\mathcal{T}_i$ and CDS_s are queried through Test. We have the following items:

$$\begin{aligned}\frac{\lambda}{2} \leq Pr[E_{SK}] &= Pr[E_{SK} \wedge E^T_{Tst}] \\ &+Pr[E_{SK} \wedge E^{CDS}_{Tst} \wedge E_t] \\ &+Pr[E_{SK} \wedge E^{CDS}_{Tst} \wedge \neg E_t]\end{aligned} \tag{12}$$

$$\begin{aligned}Pr[E_{SK}] = Pr[E_{SK} \wedge E^T_{Tst}] + Pr[E_{SK} \\ \wedge E^{CDS}_{Tst} \wedge E_t] \leq \frac{\lambda}{2} - Pr[E_t]\end{aligned} \tag{13}$$

Since
$Pr[E^{CDS}_{Tst} \wedge \neg E_t = E^T_{Tst}]$
Therefore,

$$Pr[SK = T_{n_4}(M_1)\ mod\ P] \geq \frac{\lambda}{4} - Pr[\frac{E_t}{2}] \tag{14}$$

6. Performance evaluation and comparison

This section is presented to evaluate and compare the performance of the proposed protocol with some existing protocols. Firstly, the performance of the proposed protocol is evaluated and then compared with some existing RFID-based schemes including Kumar et al. [59], Safkhani et al. [62], Anandhi et al. [67] and Jangirala et al. [61].

Table 3
Computation Time of Respective Cryptographic Operations.

Operation	Computation Time	
	Arduino Device	Cloud Server
$T_{h(.)}$	1.354 ms	0.040 ms
T_m	1.652 ms	0.063 ms
$T_{e/d}$	1.401 ms	0.052 ms

The metrics of evaluating the performance include communication cost, computation cost, and provision of security features. The details of communication cost analysis, computation cost analysis, and security features comparison are elaborated in subsequent subsections.

6.1. Computation cost analysis

This section solicits the comparison of computation cost among proposed, and related protocols [59,61,62,67].

The computation cost indicates the running time of cryptographic operations that are used in a protocol. To get the execution time of proposed and analogous protocols, we have implemented only those cryptographic operations that have been used at $\mathcal{T}_i$ and CDS_s end during the login and authentication phase of proposed and related protocols. The cryptographic operations that have been used at $\mathcal{T}_i$ end including one way hash function $T_{h(.)}$, point multiplication T_m and symmetric encryption/decryption $T_{e/d}$ are implemented on Arduino device. The specifications of the Arduino device are as follows: (i) System: Micro-controller: ATmega328 ii) RAM: SRAM 2KB iii) Clock speed: 16MHz and iv) IDE: Arduino IDE. On the other hand, cryptographic operations used at CDS_s side are implemented on an online cloud named python anywhere. The execution time of each cryptographic operation is presented in Table 3.

After getting the execution time of each cryptographic operation as mentioned in Table 3, we calculate the computation time of our protocol in the following way: $\mathcal{T}_i$ executes one-way hash function $h(.)$ for three times. The $h(.)$ used at $\mathcal{T}_i$ end is implemented on the Arduino device and its unit execution time is 1.354 ms.

Therefore, the computation cost of $\mathcal{T}_i$ side is $3T_{h(.)} \approx 4.062$ ms. Similarly, CDS_s also executes only the one-way hash function for four times and its execution time is 0.040 ms. So, the overall execution time of CDS_s side is $4T_{h(.)} \approx 0.160$ ms. Therefore, the aggregated computation cost of the proposed protocol is 4.222 ms.

The computation cost of related protocols including Kumar et al. [59], Safkhani et al. [62], Anandhi et al. [67] and Jangirala et al. [61] is also determined in the same way which is 8.751 ms, 10.435 ms, 8.324 ms and 4.930 ms, respectively. The proposed and related protocols aggregated and entity-wise computation costs are shown in Table 4. Furthermore, the graphical overview of this comparison is presented in Fig. 6. From Table 4 and Fig. 6 it is clear that our protocol requires least amount of time to complete the authentication cycle.

6.2. Communication cost analysis

This section presents the comparison of communication cost among proposed and related RFID-based authentication protocols [59,61,62,67]. The communication cost represents the number of bits they are required to transmit the messages among the participating entities of an authentication protocol. In this section, we have only considered the messages of the login and authentication phase of proposed and related protocols to accomplish the calculations of communication cost. To calculate the communication cost, we take the following assumptions: timestamp, random number, identity, point multiplication, chaotic map function, XoR, and concatenation are assumed of 160 bits in its length. Further, we assume that one-way hash function and symmetric encryption/decryption take 256 and 128 bits, respectively.

Table 4
Computation Cost Analysis.

Protocols	$\mathcal{T}_i$ End	CDS_s End	Total Computation Cost
Our	$3T_{h(.)} \approx 4.062$ ms	$4T_{h(.)} \approx 0.016$ ms	4.222 ms
[59]	$5T_{h(.)} + 1T_m \approx 8.402$ ms	$4T_{h(.)} + 3T_m \approx 0.0349$ ms	8.751 ms
[62]	$4T_{h(.)} + 3T_m \approx 10.312$ ms	$7T_{h(.)} + 7T_m \approx 0.124$ ms	10.436 ms
[67]	$6T_{h(.)} \approx 8.124$ ms	$5T_{h(.)} \approx 0.2$ ms	8.324 ms
[61]	$5T_{h(.)} \approx 6.770$ ms	$4T_{h(.)} \approx 0.160$ ms	4.930 ms

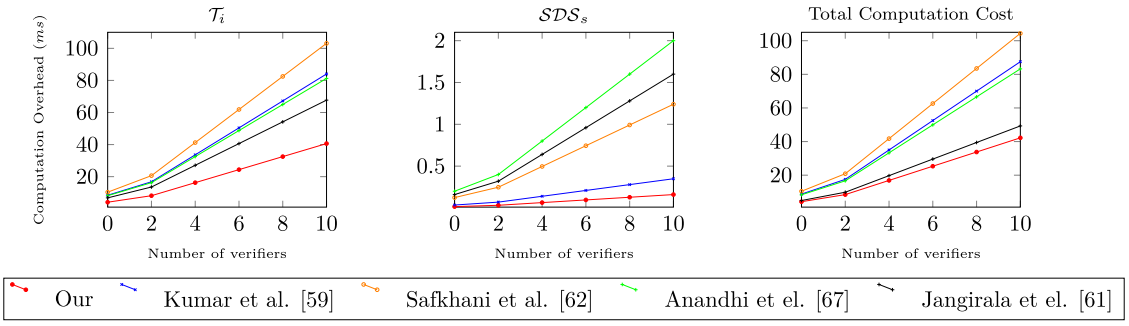

Fig. 6. Representation of aggregated computation overhead.

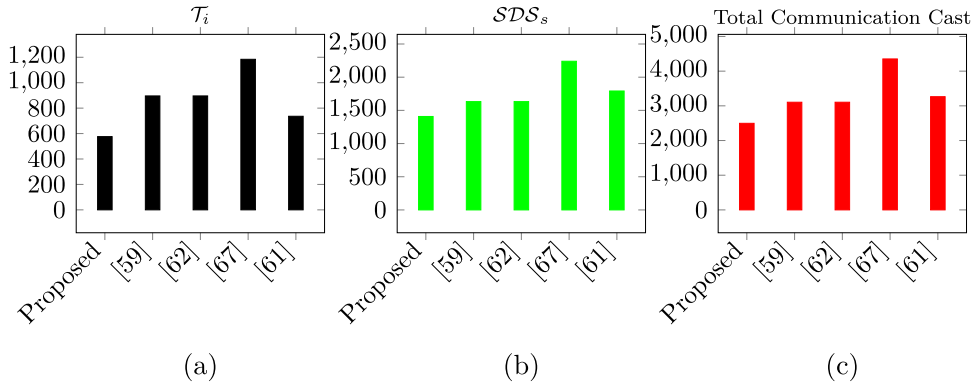

Fig. 7. Communication cost comparison.

Table 5
Communication cost analysis.

Protocols	$\mathcal{T}_i$ End	$\mathcal{R}_j$ End	CDS_s End	Total Communication Cost
Our	576 bits	1408 bits	512 bits	2496 bits
[59]	896 bits	1632 bits	576 bits	3104 bits
[62]	896 bits	1632 bits	576 bits	3104 bits
[67]	1184 bits	2240 bits	928 bits	4352 bits
[61]	736 bits	1792 bits	736 bits	3264 bits

The communication cost of proposed protocol is determined as follows: $\mathcal{T}_i$ transmits a message $\{PID_i, M_1, M_2\}$ towards $\mathcal{R}_j$, PID_i is pseudo identity, whereas $M_1 = T_{n_3}(x)\ mod\ P$ and $M_2 = h(id_i \| M_1 \| X_i)$. Therefore, the communication cost of this message is (160+160+256)= 576 bits. Whereas, $\mathcal{R}_j$ relays two messages $\{PID_i, M_1, M_2, id_j\}$ and $\{M_4, M_5, id_j\}$ towards CDS_s and $\mathcal{T}_i$, respectively. Their communication cost is (160+160+256+160)= 736 bits and (256+256+160)= 672 bits, respectively and 1408 bits collectively. Likewise, CDS_s transmits a message $\{M_4, M_5\}$ towards $\mathcal{R}_j$, where $M_4 = h(id_i \| PID_s) \oplus (M_3 \| PID_i^{i+1})$ and $M_5 = h(id_{ui} \| PID_s \| SK \| M_3 \| X_i)$. Therefore, the communication cost of message $\{M_4, M_5\}$ is (256+256)= 512 bits. Thus, the aggregated communication cost of proposed protocol is (576+1408+512)= 2496 bits. The communication cost of related protocols including Kumar et al. [59], Safkhani et al. [62], Anandhi et al. [67] and Jangirala et al. [61] is also calculated in the same way which is 3104, 3104, 4352 and 3264 bits, respectively. The Table 5 highlights the detailed comparison of entity wise and overall communication comparison among proposed and related protocols. Moreover, the graphical overview of this comparison is presented in Fig. 7. The facts of Fig. 7 are evident that our protocol incurs least numbers of bits to exchange message than all competing protocols [59,61,62,67].

6.3. Security features analysis

This section presents the comparison of security features owned by proposed and related protocols. The proposed protocol not only provides tag anonymity and perfect forward/backward secrecy but also resits major security attacks including tag impersonation, cloud data server impersonation, and ESL attacks. However, it can be seen from Table 6 that related protocols of Kumar et al. [59], Safkhani et al. [62], Anandhi et al. [67] and Jangirala et al. [61] fail to resist well-known security breaches like desynchronization attacks and ESL attack. Therefore, it is obvious from Table 6 that our protocol is secure as compared to related protocols [59,61,62,67].

The discussion of Sections 6.1–6.3 proves the supremacy of the proposed protocol over other related protocols in terms of computation cost, communication cost, and security features comparison.

7. Conclusion

The RFID-enabled systems are offering crucial approaches in the environment of networking. It is dominating the evolution of communication systems. It offers the advantages of automatic and low-cost

Table 6
Security features comparison.

Attribute	Our	[59]	[62]	[67]	[61]
$SF1$	✓	✓	✓	✓	✓
$SF2$	✓	✓	✓	✓	✓
$SF3$	✓	✓	✓	✓	✓
$SF4$	✓	✗	✗	✗	✗
$SF5$	✓	N/A	N/A	✗	✗
$SF6$	✓	✗	✗	✗	✗

$SF1$: Tag privacy and anonymity; $SF2$: Tag impersonation attack resilience $SF3$: Cloud data server impersonation attack resilience; $SF4$: ESL attack resilience; $SF5$: Perfect and backward forward secrecy; $SF6$: Desynchronization attack resilience.
✓: Provides the attribute; ✗: does not provide the attribute.

identification. However, the RFID-based systems suffer from privacy, forgery, and security issues due to the features of employing low and small frequency. The literature has keenly observed some flaws like cost, privacy, authentication, various attacks in vehicular cloud computing environment protections and maintaining communication. In order to remove all these flaws, we have proposed an ECC-based lightweight, secure, and efficient key agreement authentication protocol with essential requirements like secure cryptographic operations. In this article, we present an identity-based secure authentication scheme for the environment of vehicular cloud computing which employs an RFID system. The security of the devised scheme is scrutinized and proved formally through the well-known Random Oracle Model. The informal security analysis shows that the presented scheme has a vigorous ability to resist major attacks. We have analyzed the performance of the devised scheme and compared it with various related schemes. This comparison shows that our scheme is secure, agile, and efficient as compared to various related protocols. We will simulate our protocol in the NS3 to estimate its performance according to the distinct network perspective (e.g., throughput and end-to-end delay).

CRediT authorship contribution statement

Waseem Akram: Writing – original draft, Writing – review & editing, Informal analysis. **Khalid Mahmood:** Validation, Formal analysis. **Xiong Li:** Conceptualization, Writing – original draft, Writing – review & editing. **Mazhar Sadiq:** Performance Analysis, Comparison. **Zhihan Lv:** Investigation, Visualization, Validation. **Shehzad Ashraf Chaudhry:** Supervision, Cryptanalysis, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] S. Olariu, I. Khalil, M. Abuelela, Taking VANET to the clouds, Int. J. Pervasive Comput. Commun. (2011).
[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETS): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.
[3] S.A. Chaudhry, Designing an efficient and secure message exchange protocol for internet of vehicles, Secur. Commun. Netw. 2021 (2021) 1–9, http://dx.doi.org/10.1155/2021/5554318.
[4] N. Tekbiyik, E. Uysal-Biyikoglu, Energy efficient wireless unicast routing alternatives for machine-to-machine networks, J. Netw. Comput. Appl. 34 (5) (2011) 1587–1614.
[5] J. Wang, Y. Liu, Y. Jiao, Building a trusted route in a mobile ad hoc network considering communication reliability and path length, J. Netw. Comput. Appl. 34 (4) (2011) 1138–1149.
[6] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, J. Netw. Comput. Appl. 40 (2014) 325–344.
[7] D. Mishra, V. Kumar, S. Mukhopadhyay, A pairing-free identity based authentication framework for cloud computing, in: International Conference on Network and System Security, Springer, 2013, pp. 721–727.
[8] S. Singh, Y.-S. Jeong, J.H. Park, A survey on cloud computing security: Issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222.
[9] S. Ting, S.K. Kwok, A.H. Tsang, W.B. Lee, Critical elements and lessons learnt from the implementation of an RFID-enabled healthcare management system in a medical organization, J. Med. Syst. 35 (4) (2011) 657–669.
[10] S.F. Wamba, A. Anand, L. Carter, A literature review of RFID-enabled healthcare applications and issues, Int. J. Inf. Manage. 33 (5) (2013) 875–891.
[11] Y. Xiao, X. Shen, B. Sun, L. Cai, Security and privacy in RFID and applications in telemedicine, IEEE Commun. Mag. 44 (4) (2006) 64–72.
[12] A. Kumari, M. Yahya Abbasi, V. Kumar, A.A. Khan, A secure user authentication protocol using elliptic curve cryptography, J. Discrete Math. Sci. Cryptogr. 22 (4) (2019) 521–530.
[13] K. Srivastava, A.K. Awasthi, S.D. Kaul, R. Mittal, A hash based mutual RFID tag authentication protocol in telecare medicine information system, J. Med. Syst. 39 (1) (2015) 1–5.
[14] C.-T. Li, C.-Y. Weng, C.-C. Lee, A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system, J. Med. Syst. 39 (8) (2015) 1–8.
[15] H. Ning, H. Liu, J. Mao, Y. Zhang, Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems, IET Commun. 5 (12) (2011) 1755–1768.
[16] S.I. Ahamed, F. Rahman, E. Hoque, ERAP: ECC based RFID authentication protocol, in: 2008 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, IEEE, 2008, pp. 219–225.
[17] S.I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, T. Nakajima, Secure and efficient tag searching in RFID systems using serverless search protocol, Int. J. Secur. Appl. 2 (4) (2008) 57–66.
[18] Y. Tian-tian, F. Quan-yuan, A security RFID authentication protocol based on hash function, in: 2009 International Symposium on Information Engineering and Electronic Commerce, IEEE, 2009, pp. 804–807.
[19] C. Lv, H. Li, J. Ma, M. Zhao, Security analysis of two recently proposed RFID authentication protocols, Front. Comput. Sci. China 5 (3) (2011) 335–340.
[20] Y.-Y. Chen, J.-C. Lu, S.-I. Chen, J.-K. Jan, A low-cost RFID authentication protocol with location privacy protection, in: 2009 Fifth International Conference on Information Assurance and Security, Vol. 2, IEEE, 2009, pp. 109–113.
[21] Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. 18 (2014) 133–146.
[22] R. Peeters, J. Hermans, Attack on liao and hsiao's secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, IACR Cryptol. EPrint Arch. 2013 (2013) 399.
[23] J.-S. Chou, An efficient mutual authentication RFID scheme based on elliptic curve cryptography, J. Supercomput. 70 (1) (2014) 75–94.
[24] M.S. Farash, Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography, J. Supercomput. 70 (2) (2014) 987–1001.
[25] M. Naeem, S.A. Chaudhry, K. Mahmood, M. Karuppiah, S. Kumari, A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things, Int. J. Commun. Syst. 33 (13) (2020) e3906.
[26] S. Izza, M. Benssalah, K. Drouiche, An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment, J. Inf. Secur. Appl. 58 (2021) 102705.
[27] G. Yan, D.B. Rawat, B.B. Bista, Towards secure vehicular clouds, in: 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, IEEE, 2012, pp. 370–375.
[28] J.-L. Tsai, N.-W. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services, IEEE Syst. J. 9 (3) (2015) 805–815.
[29] D. He, N. Kumar, M.K. Khan, L. Wang, J. Shen, Efficient privacy-aware authentication scheme for mobile cloud computing services, IEEE Syst. J. 12 (2) (2016) 1621–1631.
[30] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET, IEEE Trans. Veh. Technol. 65 (2) (2015) 896–911.
[31] Y. Liu, Y. Wang, G. Chang, Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm, IEEE Trans. Intell. Transp. Syst. 18 (10) (2017) 2740–2749.
[32] Q. Jiang, J. Ni, J. Ma, L. Yang, X. Shen, Integrated authentication and key agreement framework for vehicular cloud computing, IEEE Netw. 32 (3) (2018) 28–35.
[33] W. Shi, P. Gong, A new user authentication protocol for wireless sensor networks using elliptic curves cryptography, Int. J. Distrib. Sens. Netw. 9 (4) (2013) 730831.
[34] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 14 (6) (2014) 10081–10106.
[35] S. Yu, J. Lee, K. Lee, K. Park, Y. Park, Secure authentication protocol for wireless sensor networks in vehicular communications, Sensors 18 (10) (2018) 3191.

[36] X. Liu, R. Zhang, Q. Liu, A temporal credential-based mutual authentication with multiple-password scheme for wireless sensor networks, PLoS One 12 (1) (2017) e0170657.
[37] S. Kumari, H. Om, Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines, Comput. Netw. 104 (2016) 137–154.
[38] P. Vijayakumar, M. Azees, A. Kannan, L.J. Deborah, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2015) 1015–1028.
[39] L. Kocarev, S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, Vol. 354, Springer Science & Business Media, 2011.
[40] D. Xiao, X. Liao, K. Wong, An efficient entire chaos-based scheme for deniable authentication, Chaos Solitons Fractals 23 (4) (2005) 1327–1331.
[41] G. Alvarez, Security problems with a chaos-based deniable authentication scheme, Chaos Solitons Fractals 26 (1) (2005) 7–11.
[42] D. Xiao, X. Liao, S. Deng, A novel key agreement protocol based on chaotic maps, Inform. Sci. 177 (4) (2007) 1136–1142.
[43] L. Han, Q. Xie, W. Liu, S. Wang, A new efficient chaotic maps based three factor user authentication and key agreement scheme, Wirel. Pers. Commun. 95 (3) (2017) 3391–3406.
[44] S.A. Chaudhry, M.S. Farash, N. Kumar, M.H. Alsharif, PFLUA-DIoT: A pairing free lightweight and unlinkable user access control scheme for distributed IoT environments, IEEE Syst. J. 16 (1) (2022) 309–316, http://dx.doi.org/10.1109/JSYST.2020.3036425.
[45] T.-F. Lee, C.-H. Hsiao, S.-H. Hwang, T.-H. Lin, Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps, Plos One 12 (7) (2017) e0181744.
[46] Y. Liu, K. Xue, An improved secure and efficient password and chaos-based two-party key agreement protocol, Nonlinear Dynam. 84 (2) (2016) 549–557.
[47] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li, A. Alelaiwi, Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy, Nonlinear Dynam. 83 (4) (2016) 2085–2101.
[48] X. Li, F. Wu, M.K. Khan, L. Xu, J. Shen, M. Jo, A secure chaotic map-based remote authentication scheme for telecare medicine information systems, Future Gener. Comput. Syst. 84 (2018) 149–159.
[49] S. Ahmed, S. Shamshad, Z. Ghaffar, K. Mahmood, N. Kumar, R.M. Parizi, K.-K.R. Choo, Signcryption based authenticated and key exchange protocol for EI-based V2G environment, IEEE Trans. Smart Grid 12 (6) (2021) 5290–5298.
[50] M. Umar, S.H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, M.A. Saleem, Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF, IEEE Trans. Veh. Technol. 70 (11) (2021) 12158–12167.
[51] S. Shamshad, M.S. Obaidat, M.A. Saleem, U. Shamshad, K. Mahmood, et al., Security analysis on an efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks, in: 2021 International Conference on Artificial Intelligence and Smart Systems, ICAIS, IEEE, 2021, pp. 1754–1759.
[52] S. Shamshad, M.A. Saleem, M.S. Obaidat, U. Shamshad, K. Mahmood, M.F. Ayub, On the security of a lightweight privacy-preserving authentication protocol for VANETs, in: 2021 International Conference on Artificial Intelligence and Smart Systems, ICAIS, IEEE, 2021, pp. 1766–1770.
[53] K. Mahmood, S. Shamshad, S. Kumari, M.K. Khan, M.S. Obaidat, Comment on "lightweight secure message broadcasting protocol for vehicle-to-vehicle communication", IEEE Syst. J. 15 (1) (2020) 1366–1368.
[54] S.A. Chaudhry, A. Irshad, M.A. Khan, S.A. Khan, S. Nosheen, A.A. AlZubi, Y.B. Zikria, A lightweight authentication scheme for 6G-IoT enabled maritime transport system, IEEE Trans. Intell. Transp. Syst. (2021) 1–10, http://dx.doi.org/10.1109/TITS.2021.3134643.
[55] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M.A. Lodhi, S.H. Islam, An enhanced and provably secure multi-factor authentication scheme for internet-of-multimedia-things environments, Comput. Electr. Eng. 88 (2020) 106888.
[56] G. Sriram, Security challenges of vehicular cloud computing, Int. Res. J. Modernization Eng. Technol. (2022).
[57] S.A. Chaudhry, J. Nebhen, A. Irshad, A.K. Bashir, R. Kharel, K. Yu, Y.B. Zikria, A physical capture resistant authentication scheme for the internet of drones, IEEE Commun. Stand. Mag. 5 (4) (2021) 62–67, http://dx.doi.org/10.1109/MCOMSTD.0001.2100006.
[58] Z. Ali, A. Ghani, I. Khan, S.A. Chaudhry, S.H. Islam, D. Giri, A robust authentication and access control protocol for securing wireless healthcare sensor networks, J. Inf. Secur. Appl. 52 (2020) 102502.
[59] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, M.K. Khan, RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing, Veh. Commun. 22 (2020) 100213.
[60] S.A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, Y.B. Zikria, Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment, ACM Trans. Internet Technol. (TOIT) 21 (3) (2021) 1–19.
[61] S. Jangirala, A.K. Das, A.V. Vasilakos, Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment, IEEE Trans. Ind. Inf. 16 (11) (2019) 7081–7093.
[62] M. Safkhani, C. Camara, P. Peris-Lopez, N. Bagheri, RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing, Veh. Commun. 28 (2021) 100311.
[63] A. Irshad, M. Sher, H.F. Ahmad, B.A. Alzahrani, S.A. Chaudhry, R. Kumar, An improved multi-server authentication scheme for distributed mobile cloud computing services, KSII Trans. Internet Inf. Syst. (TIIS) 10 (12) (2016) 5529–5552.
[64] T. Maitra, M.S. Obaidat, R. Amin, S.H. Islam, S.A. Chaudhry, D. Giri, A robust elgamal-based password-authentication protocol using smart card for client-server communication, Int. J. Commun. Syst. 30 (11) (2017) e3242.
[65] X. Li, F. Wu, S. Kumari, L. Xu, A.K. Sangaiah, K.-K.R. Choo, A provably secure and anonymous message authentication scheme for smart grids, J. Parallel Distrib. Comput. 132 (2019) 242–249.
[66] M. Abdalla, P.-A. Fouque, D. Pointcheval, Password-based authenticated key exchange in the three-party setting, in: International Workshop on Public Key Cryptography, Springer, 2005, pp. 65–84.
[67] S. Anandhi, R. Anitha, V. Sureshkumar, An authentication protocol to track an object with multiple RFID tags using cloud computing environment, Wirel. Pers. Commun. 113 (4) (2020) 2339–2361.

Waseem Akram is currently working as a lecturer with the Department of Computer Science (CS) at Lahore Garrison University, Main campus, Lahore, Pakistan. He has done his MS (CS) from the Islamia University Bahawalpur, Baghdad-ul-Jadeed Campus, Pakistan. He received his BS(CS) from COMSATS University Islamabad in 2017. His research interests include remote user authentication and key agreement in IoMT environments.

Khalid Mahmood received the Ph.D. degree in computer science from the International Islamic University, Islamabad, Pakistan, in 2018. He is currently working as an Assistant Professor at the Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin, Taiwan. Earlier, he also served as a Faculty Member with COMSATS University Islamabad, which is ranked no. 1 in the IT category. He has published more than 55 SCI/E indexed articles and has been cited more than 1000 times. He is an approved supervisor by the Higher Education Commission of Pakistan. He has supervised more than 15 graduate students in their research. His research interests include design and development of lightweight authenticated and key agreement solutions for diverse infrastructures like smart grid, the Internet of Drones (IoD), the Internet of Things (IoT), vehicular ad hoc networks (VANET), mobile edge computing, and blockchain. In 2017, considering his research, Pakistan Council for Science and Technology granted him the Prestigious Young Productive Scientist Award, while affirming him among Top Productive Computer Scientists in Pakistan.

Xiong Li now is an associate professor at School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. He received his master's degree in mathematics and cryptography from Shaanxi Normal University (SNNU), China in 2009 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT), China in 2012. He has published more than 40 referred journal papers in his research interests, which include cryptography and information security, etc. He has served on TPC member of several international conferences on information security and reviewer for more than 20 ISI

indexed journals. He is a winner of the 2015 Journal of Network and Computer Applications Best Research Paper Award.

Mazhar Sadiq was born in Pakistan. He received the bachelor's and master's degrees in computer science from Pakistan, the Master of Science degree from Blekinge Institute of Technology, Sweden, in 2007, and the Ph.D. degree from the University of Jyvaskyla, Finland, in 2016. After completing the master's degree, he went to Sweden for higher education. Since March 2017, he has been working as an Assistant Professor with COMSATS University Islamabad– Sahiwal, Sahiwal, Pakistan. He has taught human– computer interaction and machine learning courses to bachelor level students. He has supervised many master of computer science students. He is the author of more than ten articles. His research interests include usability, virtual reality, machine learning, and augmented reality.

Zhihan Lv (Senior Member, IEEE) received the Ph.D. degree in computer applied technology from Ocean University of China, Qingdao, China, in 2012. He is currently associated with Department of Game design, Faculty of Arts, Uppsala University, Sweden. He has completed several projects successfully on PC, Website, smartphone, and smartglasses. His research interests include big data analytics, multimedia, augmented reality, virtual reality, computer vision, 3- D visualization and graphics, serious game, HCI, bigdata, and GIS.

Shehzad Ashraf Chaudhry received the master's and Ph.D. degrees (with Distinction) from International Islamic University Islamabad, Pakistan, in 2009 and 2016, respectively. He is currently working as an Associate Professor of Cybersecurity Engineering, Abu Dhabi University, Abu Dhabi, UAE. He is also holding an adjunct Associate Professorship with Nisantasi University Istanbul, Turkey. He has authored over 150 scientific publications appeared in different international journals and proceedings, including more than 120 in SCI/E journals. Some of his works are published at top venues like IEEE Transaction on Industrial Informatics, IEEE Transactions on Intelligent Transportation Systems, IEEE Internet of Things Journal, IEEE Transactions on Reliability, IEEE Transactions on Industry Applications, IEEE Systems Journal, ACM Transaction on Internet Technology, Elsevier's Sustanable Cities and Scoieties, Computer Networks, Sustainable Energy Technologies and Assessments, Computer Communications etc. With an H-index of 38 and an I-10 index 77, his work has been cited over 3800 times. He has also supervised over 40 graduate students in their research. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystem, and next generation networks. He occasionally writes on issues of higher education in Pakistan. Dr. Chaudhry was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. For the consecutive two years, he is being listed among Top 2% Computer Scientists across the world in Stanford University's reports.