Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **7**, Number **3**, August **2022**

RAVCC: Robust Authentication Protocol for RFID based Vehicular Cloud Computing

Vikas Kumar

Department of Mathematics,
SSV College, Hapur, Uttar Pradesh-245101, India
vikas.chaudhary26@gmail.com

Rahul Kumar

Department of Mathematics,
SSV College, Hapur, Uttar Pradesh-245101, India
ujjwalrahul@gmail.com

Vinod Kumar

Department of Mathematics,
PGDAV College, University of Delhi 110065, India
vinod.iitkgp13@gmail.com, vinod@pgdav.du.ac.in

Adesh Kumari

Department of Mathematics,
Dyal Singh College, University of Delhi 110003, India
adeshbhucker@gmail.com

Saru Kumari*

Department of Mathematics,
Chaudhary Charan Singh University, Meerut-250004, India
saryusiirohi@gmail.com

*Corresponding author: Saru Kumari

Received February 21, 2022, revised March 24, 2022, accepted May 20, 2022.

Abstract. *Vehicular cloud computing (VCC) stands for vehicle cloud computing, which combines cloud, vehicular networking, and Internet of Things (IoT) and related technologies. VCC is defined as vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-device communication in which vehicles have communication sensing capabilities. Vehicle resources, cloud infrastructure, and the Internet of Things are all used by VCC. VCC, on the other hand, places a premium on communication security and the privacy of communicators. We present an ECC based authentication framework for Radio Frequency Identification (RFID) based on VCC, which is equipped with a radio frequency identification, to meet the goal of safe communication while maintaining anonymity. To prove the claim of safe communication, we employ formal security analysis in the random oracle model, BAN logic and informal analysis. On the basis of desirable performance parameters, we explain and evaluate the performance of the suggested framework, as well as compare it to similar systems. The proposed architecture, according to our findings, provides all needed security criteria while also permitting effective communication.*
Keywords: Vehicular cloud computing, Elliptic curve cryptography, Authentication, Security and privacy, Radio Frequency Identification.

1. **Introduction.** The researchers were able to analyse and test a wide range of network applications in a variety of scenarios thanks to advancements in " hardware, software, and transmission infrastructure". The Vehicular Ad-Hoc Network (VANET) is a new paradigm for transferring information in a traditional network of automobiles that has gained a lot of attention in recent years [1, 2]. VCC's goal is to provide real-time computing capabilities to vehicles with limited computer capabilities, reducing travel time, avoiding accidents, and reducing traffic congestion. thus, the technology's adoption will be good for the environment. Furthermore, VCC allows for the theoretical integration of " Wireless Sensor Networks, Mobile Cloud Computing, and Intelligent Transportation Systems"for better road safety and a well-informed urban transportation system [3, 4]. In VCC, network connections from vehicles to infrastructure (V2I) or vehicles to vehicles (V2V) connect each vehicle to the other vehicle or to the network communication infrastructures [5]. Collaboration as a service, development as a service, storage as a service, network as a service, computing as a service, information as a service, mobile backend as a service, pictures on a wheel as a service, platform as a service, entertainment as a service, infrastructure as a service, function as a service, and data as a service are some of the cloud services used by the VCC. The VCC communication domain is accessible as Platform as a Service. This application can be used for a variety of tasks, such as gathering information about nearby base stations and roadside units, collecting traffic data, sending emergency message/call alerts, managing staff availability, and maintaining an intelligent and skilled environment by utilising user feedback based on previous data. The cloud makes it easier to acquire, process, and manage user data in this environment. The cloud is considered to be in sync with the roadside unit's base stations, which is where the client's real-world security issues manifest [6].

RFID is a widely used technique for object identification. This technique was used to identify and distinguish between enemy and friendly weapons during World War II. Because of its numerous applications, this technology has grown rapidly to date. Among the applications are "airport baggage tracking logistics, tracking and billing procedures, commodities tracking, machine-readable travel papers, smart dust, individual and animal monitoring, toll collection, contactless payment, access management, and a variety of others " [7, 8, 9]. Some of the most frequent RFID applications are "passport identification, healthcare systems, management systems, and luggage identification at airports" [7]. The classic barcode architecture has been replaced by contactless item identification as a result of RFID application [7, 9]. Client information is captured by vehicles equipped with low-frequency interrogators/readers within a specified number of different networks. The RFID-reader delivers services in the event of " damage, accidents, vehicle unavailability or emergencies, as well as managing increased error tolerance in networks". The facility is provided to the consumer on wheels using RFID-based technology [10, 11, 12, 13, 14]. To collect client data, vehicles are linked to RFID-based devices in VANETs. As the population grows, more dedicated resources are required, as well as efficient services for people on wheels. As a result, developing a safe, efficient, and dependable RFID based VCC architecture is a good appoarch. Many academics have recently presented anonymous and mutual authentication solutions for VCC. However, RFID-based VCC systems have received little attention. The RFID tag must be reported as anonymous in these systems. Anonymity and un-linkability are required to maintain the privacy of the tag and the reader [15, 16].

1.1. **Related work.** The following is a summary of the literature review for the suggested procedure as presented in this portion of the paper. A security concern for car cloud computing was proposed by Yan et al. [17]. They created a VCC architecture that

provides security and privacy in the vehicle environment to overcome basic problems. This was the first study that discussed VCC's security issues. Tsai and Lo [18] proposed an authentication technique for mobile-based cloud computing that is both efficient and private. They asserted that the suggested technique is safe and secure, and that it authenticates both the service provider and the user. Tsai and Lo's approach has security weaknesses, including as an impersonation attack, according to He et al. [19]. He et al. developed a mobile cloud computing authentication mechanism that was more secure. Sharma et al. [20] developed a vehicle cloud computing architecture with a dynamic key feature. The method devised by Sharma et al. had major security weaknesses, including traceability and forward secrecy. Wang et al. [21] proposed a two-party lightweight authentication scheme. In the proposed technique, Liu et al. were able to revoke the user functionality while also lowering the communication overhead. However, as they claimed, the total scheme's computing time did not decrease significantly. Liu et al. proposed an important agreement protocol for the internet of vehicle [22]. The suggested approach, according to Liu et al., is effective for vehicular-to-vehicle authenticated communication. The security of vehicle network connectivity was also improved. For automotive cloud computing, Jiang et al. [23] developed a non-interactive key agreement system. The technique proposed is based on identification and incorporates vehicle authentication in a cloud environment. However, greater communication overhead is required to achieve this. Shi et al. suggested an ECC-based user authentication system for wireless sensor networks (WSNs) that is immune to " insider attacks, off-line password guessing assaults, anonymity, parallel session attacks, and untraceable attacks" [24]. Choi et al. [25] established a secure user authentication system for WSNs based on the ECC protocol that does not include anonymity, mutual authentication, impersonation, untraceable attack, or a password changing phase. Vijayakumar et al. suggested a system for vehicle ad-hoc communications that is both secure and efficient [26].

1.2. **Motivation and contribution.** Various authentication methods [9, 27, 28, 15, 12, 13] for VCC and RFID systems have been devised in the previous decades, according to our understanding and based on the existing literature. For RFID-based VCC systems, however, authenticated key agreement procedures are missing. Because RFID and VCC have differing computing capacities and privacy needs, authenticated key agreements are required in RFID assisted VCC systems. We provide an ECC-based authenticated key agreement technique for RFID-assisted VCC systems as a result. Some of the key features of the proposed scheme are as follows:

- The key formed between the RFID-tag and the VC database server is backed up by the authentication process.
- RAVCC scheme's security is demonstrated both formally and informally.
- Tag and cloud server compute a common session key and agree on it.
- The performance study and comparative results reveal that RAVCC has desirable performance characteristics.

1.2.1. ***Layout of the paper***. The following is the rest of the paper's layout: The preliminary data is found in Section 2. The system model is covered in Section 3. Section 4: Using RFID to provide a safe and effective authentication framework for cloud infrastructure for vehicles (RAVCC). Security investigation section 5 of the RAVCC. The performance of the suggested protocol is discussed in section 6. Finally, we'll go over the conclusion. Table 1's notations are also used.

2. Preliminaries.

TABLE 1. Notations

Symbol	Description	Symbol	Description
T_i, R_j & S	i^{th} RFID tag, j^{th} RFID reader & VC server	PW_T	Password of i^{th}
SUL	The simulator	s	Secret key of S
$\mathcal{E}(F_q)$	Elliptic curve $\mathcal{E}$ over a prime finite field F_q	$\triangle T$	Communication's maximum time delay
l	The parameter for security	F_q	The order's prime finite field q
q	Large prime	$\oplus$	Operation of bitwise XOR
ID_i	The i^{th} participant's identity	$\|$	Concatenation operation
G	Additive group of Elliptic curve points	g	Base point of G
$h(\cdot)$	Cryptographic one way hash function	Z_q^*	Group under multiplication with order $q-1$
$SK_{ij}(.)$	Entities i and j share a session key	$i \stackrel{?}{=} j$	Whether i and j are equal
VCC	The vehicular cloud computing	s_i	Serial number of i^{th} RFID tag
$\mathbb{A}$	Adversary	$\approx$	Approximate value

2.1. **The fundamentals of ECC in a finite field.** Let $E_q(i,j) : v^2 = w^3 + iw + j \bmod q$, be a non singular elliptic curve over a finite field $Z_q^\star$ where $i, j \in Z_q^\star$ with $4i^3 + 27j^2 \bmod q \neq 0$ and $G = \{(w,v) : v, w \in Z_q, (w,v) \in E\} \cup \{\theta\}$, where θ is group identity under addition [27]. The following are some operations that can be performed on G [29]:

1. Let $M = (w,v) \in G$, then define $-M = (w,-v)$ and $M + (-M) = \theta$
2. Let $M = (w,v) \in G$ then the scalar multiplication is defined as: $tM = M + M + M..... + M\ (t - times)$.
3. If $M = (w_1, v_1)$, $N = (w_2, v_2)$, then $M+N = (w_3, v_3)$, where $w_3 = \lambda^2 - w_1 - w_2\ mod\ p$ and $v_3 = \lambda(w_1 - w_2) - v_1\ mod\ q$, with

$$\lambda = \begin{cases} \frac{v_2 - v_1}{w_2 - w_1} \ \ mod \ \ \mathrm{q} \ \ if \ \ M \ \neq N \\ \\ \frac{3w_1^2 + i}{2v_1} \ \ mod \ \ \mathrm{q} \ \ if \ \ M \ = N \end{cases}$$

- "**Elliptic curve discrete logarithm problem (ECDLP)**: For inputs $M, N \in G$, computationally hard to calculate $a \in Z_q^*$ such that $N = aM$ [30]".
- "**Elliptic curve computational Diffie-Hellman problem (ECCDHP)**: Let $a, b \in Z_q^*$ and g is generator of G. For input (g, ag, bg), it is computationally hard to execute abg in G [27]".

2.2. **System model.**

2.2.1. ***Network model for RAVCC.*** The presented framework is a new method targeted at improving road and roadside infrastructure users' security and privacy. It also provides migrating clients with the necessary expertise and well-developed services as needed. The merits of the RFID system underpin the proposed paradigm. The figure 1 illustrates the architecture of the planned RAVCC.

2.2.2. ***Attack model and assumptions.*** In relation to our suggested protocol, the attack model is shown:

- An attacker $\mathbb{A}$ might try to break communication between RFID-based tags, readers, or the database server by using an insecure channel.
- $\mathbb{A}$ can use active attack, passive attack, or a combination of both to deal with the readers and the tag.
- As part of the aggressiveness process, $\mathbb{A}$ can spoof/masquerade as the suitable readers and tags by using rouge readers or tags in the structures.

We make the following basic assumptions in RAVCC:

- A RFID based waistline connected to the area network is worn by users travelling on the road/highways.
- Low-frequency RFID scanners are installed in the vehicles.

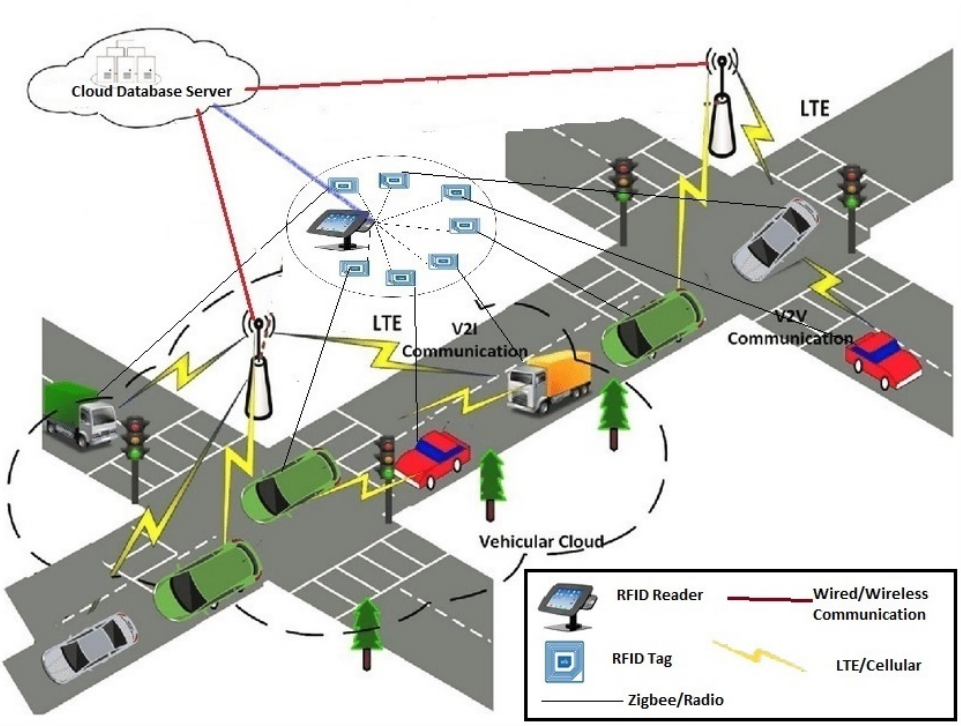

FIGURE 1. The proposed architecture for RAVCC [31]

- High-frequency RFID readers are provided on the roadside units.
- Because communication between RFID-enabled readers, tags, and the database server looks to be open, it must be secured.

2.2.3. ***Working methodology***. The cloud server, tags, and readers make up an RFID-based system. Active, semi-active, and passive RFID tags are the three types of RFID tags. In the communication system, customers utilise passive tags to identify themselves. Information is sent to the tag by the reader. The tag then provides the reader with revised information. During the authentication process, data is sent to the cloud server. In the RFID-VCC system, data is transferred across an unsecured channel. Wired or wireless networks can be used as a communication medium [27, 32, 33, 34].

TABLE 2. Tag registration phase via secure communication

Tag T_i	**Cloud database server** S
Inputs ID_T and PW_T	
Generates random value r	
Computes $PWT = h(r\|\|PW_T\|\|ID_T)$	
Sends $M_{R1} = \{PWT, ID_T\}$	
$\cdots\cdots\cdots\cdots\Rightarrow$	Generates random serial number s_i
	Computes $V_1 = h(s\|\|s_i\|\|ID_T)$, where s is secret key of S
	Computes $V_2 = h(V_1\|\|PWT\|\|ID_T)$
	Computes $V_3 = V_1 \oplus PWT$
	Sends $M_{R2} = \{V_2, V_3, s_i, g, G, h(.)\}$
	$\Leftarrow\cdots\cdots\cdots\cdots\cdots$
Store $\{V_2, V_3, s_i, g, G, h(.)\}$ in database	

3. The RAVCC framework.

3.1. **Initialization phase.** Initially, S chooses EC with the equation $v^2 = u^3 + au + b$ over $Z_q^\star$. S chooses g as the G generator from a non-singular elliptic curve. Further, S generates $s \in F_q$ and established as a secret key.

3.2. **Registration phase.**

Step RT1: To register with S, T_i inputs ID_T, PW_T, generates random value r, executes $PWT = h(r\|PW_T\|ID_T)$ and sends $M_{R1} = \{PWT, ID_T\}$ to S via secure channel.

Step RT2: On receiving M_{R1}, generates random serial number s_i. Further, S computes $V_1 = h(s\|s_i\|ID_T)$, where s is secret key of S, computes $V_2 = h(V_1\|PWT\|ID_T)$ and $V_3 = V_1 \oplus PWT$. Then, S sends $M_{R2} = \{V_2, V_3, s_i, g, G, h(.)\}$ to T via secure channel.

Step RT3: On receiving M_{R2}, T stores parameters $\{V_2, V_3, s_i, g, G, h(.)\}$ in his/her the database.

Table 2 shows the procedure used in the registration process.

3.3. **Login, authentication and key agreement phase.** T_i successfully registers with S, and when she/he wants to use the service, she/he makes an access request to S. The following is a description of the procedure:

Table 3. Phase of public channel of login and authentication

RFID Tag T_i	**RFID Reader** R_j	**Cloud database server** S
Login with ID_T^*, PW_T^* and r^*		
Computes $PWT^* = h(r^*\|PW_T^*\|ID_T^*)$		
Computes $V_1^* = V_3 \oplus PWT^*$		
Computes $V_2^* = h(V_1^*\|PWT^*\|ID_T^*)$		
Verifies $V_2^* \stackrel{?}{=} V_2$		
Generates random value x		
Computes $x' = x \oplus (V_2 \oplus s_i)$		
Computes $W_1 = h(V_3\|ID_T\|PWT\|V_2)$		
Encrypts $E_1 = E_{(V_2 \oplus V_3)}(x', W_1)$		
Sends $M_1 = \{E_1, t_1\}$		
$\cdots\cdots\cdots\cdots\rightarrow$	Verifies $t_2 - t_1 \stackrel{?}{\leq} \triangle t$	
	Sends $M_2 = \{E_1, t_3\}$	
	$\cdots\cdots\cdots\cdots\rightarrow$	Verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$
		Decrypts $(x', W_1) = D_{(V_2 \oplus V_3)}(E_1)$
		Computes $W_1^* = h(V_3\|ID_T\|PWT\|V_2)$
		Verifies $W_1^* \stackrel{?}{=} W_1$
		Computes $x^* = x' \oplus (V_2 \oplus s_i)$
		Generates random value y
		Computes $SK_{ST} = h(ID_T\|x^*yg\|s_i\|t_5)$
		Computes $y' = ((y \oplus W_1^*) \oplus (V_3 \oplus s_i))$
		Computes $W_2 = h(PWT\|x^*\|y\|t_5\|V_3)$
		Encrypts $E_2 = E_{((V_3 \oplus s_i) \oplus W_1^*))}(y', W_2, t_5)$
		Sends $M_3 = \{E_2, t_5\}$
		$\leftarrow\cdots\cdots\cdots\cdots$
	Verifies $t_6 - t_5 \stackrel{?}{\leq} \triangle t$	
	Sends $M_4 = \{E_2, t_7\}$	
	$\leftarrow\cdots\cdots\cdots\cdots$	
Verifies $t_8 - t_7 \stackrel{?}{\leq} \triangle t$		
Decrypts $(y', W_2, t_5 x', W_1) = D_{((V_3 \oplus s_i) \oplus W_1))}(E_2)$		
Computes $y^* = ((y' \oplus W_1) \oplus (V_3 \oplus s_i))$		
Computes $W_2 = h(PWT\|x\|y^*\|t_5\|V_3)$		
Verifies $W_2^* \stackrel{?}{=} W_2$		
Computes $SK_{TS} = h(ID_T\|y^*xg\|s_i\|t_5)$		

Step AF1: T_i login with ID_T^*, PW_T^* and r^*. Further, executes $PWT^* = h(r^* \| PW_T^* \| ID_T^*)$, $V_1^* = V_3 \oplus PWT^*$, $V_2^* = h(V_1^* \| PWT^* \| ID_T^*)$ and verifies $V_2^* \stackrel{?}{=} V_2$. Then, generates random value x, computes $x' = x \oplus (V_2 \oplus s_i)$, $W_1 = h(V_3 \| ID_T \| PWT \| V_2)$, encrypts $E_1 = E_{(V_2 \oplus V_3)}(x', W_1)$ and sends $M_1 = \{E_1, t_1\}$ to R_j via public channel.

Step AF2: On receiving M_1, R_j verifies $t_2 - t_1 \stackrel{?}{\leq} \triangle t$ and sends $M_2 = \{x', W_1, t_3\}$ to S via public channel.

Step AF3: On receiving M_2, S verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$. Further, S decrypts $(x', W_1) = D_{(V_2 \oplus V_3)}(E_1)$, computes $W_1^* = h(V_3 \| ID_T \| PWT \| V_2)$ and verifies $W_1^* \stackrel{?}{=} W_1$. After that, S computes $x^* = x' \oplus (V_2 \oplus s_i)$, generates random value y, computes $SK_{ST} = h(ID_T \| x^* y g \| s_i \| t_5)$, $y' = ((y \oplus W_1^*) \oplus (V_3 \oplus s_i))$, $W_2 = h(PWT \| x^* \| y \| t_5 \| V_3)$, encrypts $E_2 = E_{((V_3 \oplus s_i) \oplus W_1^*))}(y', W_2, t_5)$ and sends $M_3 = \{E_2, t_5\}$ to R_j via public channel.

Step AF4: On receiving M_3, R_j verifies $t_6 - t_5 \stackrel{?}{\leq} \triangle t$. Further, sends $M_4 = \{E_2, t_7\}$ to T_i via public channel.

Step AF5: Upon receiving M_4, T_i verifies $t_8 - t_7 \stackrel{?}{\leq} \triangle T$. Then, T_i decrypts $(y', W_2, t_5, x', W_1) = D_{((V_3 \oplus s_i) \oplus W_1))}(E_2)$, computes $y^* = ((y' \oplus W_1) \oplus (V_3 \oplus s_i))$, computes $W_2^* = h(PWT \| x \| y^* \| t_5 \| V_3)$ and verifies $W_2^* \stackrel{?}{=} W_2$. Further, set session key $SK_{TS} = h(ID_T \| y^* x g \| s_i \| t_5)$.

As a result, T_i and S agree on a session key $SK = SK_T = SK_S$ and establish mutual authentication. Table 3 depicts the login and authentication portion of the process.

4. **Security analysis.**

4.1. **Formal security evaluation.** We used a formal model for RAVCC in this part, which is based on the "random oracle model" [35, 36, 37, 7]. To make it fit for RAVCC, we make certain changes to the original. We utilise three participants $T, R, andS$ as "the tag, reader, and server", respectively, to demonstrate our proof. The identification of T is ID_T, and the password is PW_T. In the same way, identification of S is ID_S. The password dictionary is $\mathbb{N}$. More information about this model can be found in [38, 39].
For formal security analysis, we present the theorem and its proof as follows:
Theorem 1: The protocol $\sum$ operators G under multiplication q. Where, "password dictionary $\mathbb{D}$ has size $\mathbb{N}$. Here, $\mathbb{A}$ has queries: q_s send queries, q_h hash queries, and q_e execute queries" and then,
$Adv_{\sum}^{sfs-ake}(\mathbb{A}) \leq \frac{O(q_s+q_e)^2}{(q-1)} + \frac{O(q_h)^2+O(q_s+q_e)^2}{2^l} + \frac{O(q_h)+O(q_s)}{2^{l-1}} + \frac{O(q_s)}{\mathbf{N}} + O((q_h(q_s+q_e)^2+1)Adv_{\mathbb{A}}^{ECDDH}(\tau')$, Where $\tau' = t + (O(qe) + O(q_s))T_{\mathbb{M}}$ and $T_{\mathbb{M}}$ is the time which used in one scalar multiplication on G.
Proof: With the help of a game setup, we show the above theorem. We employ eight games in this example, ranging from $Game_0$ to $Game_8$. The Su_j event is $\mathbb{A}$ exact predicting the coin η by the analysis session in game $Game_j$. $\mathbb{A}$ wishes to execute ID_T and PW_T because there is only one tag T_i throughout these games. The following are the measures to take:

- $Game_0$: By definition, $Game_0$ is the accurate game for RAVCC using the random oracle model technique. Then, we have

$$Advt_{\Pi}^{sfs-ake}(\mathbb{A}) = 2Pb[Su_0] - 1 \tag{1}$$

In addition, if there are multiple occurrences, a random $\eta*$ response is used. Following is a list of some of the occurrences:
- If $\mathbb{A}$ does not guess $\eta*$, the game ends or is removed.

- $\mathbb{A}$ does more queries than the planned upper bound.
- $\mathbb{A}$ takes longer than the highest bound that is considered.

- $Game_1$: All SUL inquiries are added together in this case. The following is a list of questions that have received a response:
  - L_H: All hash queries are given a response.
  - L_P: A transcript of the computer network is mentioned
  - L_E: It displays the results of $\mathbb{A}$'s queries to two random oracles.

  In Table-4, you can see a list of all the queries. If $Game_1$ and $Game_0$ are identical using the previously provided facts,

$$Pb[Su_1] - 1 = Pb[Su_0] \tag{2}$$

- $Game_2$: In this method, we hope to find the effect of transcriptions on rejection. The probabilistic appoarch of these is explained by the birthday paradox:
  - In an unique session, you can pick $x, y, s_i \in Z_q^\star$. Then,

$$\frac{O(q_s + q_e)^2}{2(q-1)} + \frac{O(q_s + q_e)^2}{2^{l+1}}$$

  - The hash query's upper bound is $\frac{O(q_h)^2}{2^{l+1}}$.

  Except for the collisions, $Game_2$ and $Game_1$ are very identical. We can see this

$$|Pb[Su_2] - Pb[Su_1]| \leq \frac{O(q_s + q_e)^2}{2(q-1)} + \frac{O(q_h)^2 + O(q_s + q_e)^2}{2^{l+1}} \tag{3}$$

- $Game_3$: In $Game3$ Since, SUL all the answer R_J, we have chosen few steps on $Send\ (T^i, R^t, M_1)$, SUL wants to check if $M_1 \in L_P$ and $(V_3 \| ID_T \| PWT \| V_2, W_1) \in L_E$. If this fails, it will be terminated. In this way, $Game_3$ and $Game_2$ are same, we mention the probability for $\mathbb{A}$ forge M_1 commensurate. Then,

$$|Pb[Su_3] - Pb[Su_2]| \leq \frac{O(q_s + q_e)}{2^l} \tag{4}$$

- $Game_4$: We evaluate the likelihood of forging M_2 for $\mathbb{A}$ in $Game_4$. Since SUL allows for a S response, we add a few steps to $Send(R^t, S^j, M_2)$. SUL wants to see if M_2 is in L_P and (E_1, t_3) is in L_E. If this fails, the session should be terminated. $Game_4$ and $Game_3$ are similar in this sense. Then

$$|Pb[Su_4] - Pb[Su_3]| \leq \frac{O(q_s + q_e)}{2^l} \tag{5}$$

- $Game_5$: The likelihood of forging M_3 for $\mathbb{A}$ is considered below, since SUL is the reader, he contributes the response. We add few steps on $Send\ (S^j, R^t, M_3)$, SUL wants to validate if, $M_3 \in L_P$ and $(V_3 \| ID_T \| PWT \| V_2, W_1^*), (ID_T \| * \| s_i \| t_5, SK_{ST})$, $(PWT \| * \| * | t_5 \| V_3, W_2) \in L_E$. If it fails, it will be turned off. After that, $Game_5$ and $Game_4$ resemble each other. Then,

$$|Pb[Su_5] - Pb[Su_4]| \leq \frac{O(q_h + q_s)}{2^l} \tag{6}$$

- $Game_6$: We evaluate the likelihood of forging M_4 for $\mathbb{A}$ in $Game_6$. Since SUL allows for a S response, we add a few steps to Send (R^t, T^i, M_4). SUL wants to see if M_4 is in L_P and (E_3, t_3) is in L_E. If this fails, the session should be terminated. $Game_6$ and $Game_5$ are similar in this sense. Then

$$|Pb[Su_6] - Pb[Su_5]| \leq \frac{O(q_s + q_e)}{2^l} \tag{7}$$

- $Game_7$: ECGDHP is used in this case. We suppose that $\mathbb{A}$ will break the session if he can obtain the assured session key via H-oracle and be the realisation. We are modifying the H-oracle as follows: I) $\mathbb{A}$ queries $(ID_T \| * \| * \| t_5), W_2), (ID_T \| * \| * \| t_5, SK_{TS})$. Here, SUL verifies if $(ID_T \| * \| * \| t_5), W_2^*), (ID_T \| * \| * | t_5, SK_{TS}) \in L_E$. If it fails, the session key is displayed. Otherwise, To investigate $X \stackrel{?}{=} ECDDHP(xg, yg)$, SUL use the ECGDHP oracle. In this time, if the query is unsuccessful, it is discarded. Otherwise, SUL takes a $SK \in \{0,1\}^l$ output as $(ID_T \| * \| * \| t_5, SK), (ID_T \| * \| * \| t_5), W_2^*)$ to L_E.

  We investigated $Game_7$ and found that it had two forms of attacks: active and passive. During one session, the attacker requests a *Corrupt* query and obtains all communication messages:
  - E might take a password from the $\mathbb{D}$ for password guessing attacks. When $\mathbb{A}$ can dedicate *Sendquery* q_s with $\mathbb{N}$, $\mathbb{A}$ has a $\frac{q_s}{\mathbb{N}}$ chance of guessing the right password using the session.
  - In passive attacks, it's used. Two cases arose as a result of this:
    - ◇ To begin, $\mathbb{A}$ scans the message, then $\mathbb{A}$ inquires about *Execute queries*. Finally, $\mathbb{A}$ requests that H-query be completed, which violates ECGDHP. We can look for xyg. With the probability $1/Q_h$, from L_E. As a result, the probability is bounded by $q_h Advt_{\mathbb{A}}^{ECDDHP}(\tau + O(q_e)T_{\mathbb{M}})$ in this fashion.
    - ◇ In the second method, $\mathbb{A}$ looks into each of the *Send queries* requests one by one. Then, in this way, $Q_h Advt_{\mathbb{A}}^{ECDDHP}(\tau + O(q_s)T_{\mathbb{M}})$ as an upper bound.

  The probability for this is $q_h Advt_{\mathbb{A}}^{ECDDHP}(\tau + O(q_e)T_{\mathbb{M}}) + q_h Advt_{\mathbb{A}}^{ECDDHP}(\tau + O(q_s)T_{\mathbb{M}}) \leq q_h Advt_{\mathbb{A}}^{ECDDHP}(2\tau + [O(q_s) + O(q_e)]T_{\mathbb{M}})$, where $\tau' = (2\tau + [O(q_s) + O(q_e)]T_{\mathbb{M}})$. Then, we have

$$|Pb[Su_7] - Pb[Su_6]| \leq \frac{q_s}{\mathbb{N}} + \ Q_h Advt_{\mathbb{A}}^{ECDDHP}(\tau') \tag{8}$$

- $Game_8$: It is employed for complete forward security in this game. *Corrupt* queries should be queried following the *Test* query, according to the $sfs - fresh$ technique. So, $\mathbb{A}$ can only get around ancient questions and writings. We can get $(l, ID_T \| * \| * \| * \| T_{LA5}, SK)$ in L_E in this last game. The chances of receiving xg and yg in the same session is $1/(q_s + Qqe)^2$ and we have

$$|Pb[Su_8] - Pb[Su_7]| \leq q_h(q_s + q_e)^2 Advt_{\mathbb{A}}^{ECDDHP}(\tau') \tag{9}$$

Finally, after combining all of the games, using $\mathbb{A}$ to estimate the session key and $Pb[Su_8] = \frac{1}{2}$ to predict the session key is no longer beneficial. Finally, this theorem has been proven.

5. **BAN logic.** We performed security analysis utilizing the BAN logic to demonstrate the secure mutual authentication of the proposed scheme. We present the BAN logic notations in Table 2. Furthermore, we define the rules, the goals, the idealized form, and the assumptions for BAN logic analysis. We prove that the proposed scheme provides secure mutual authentication among $T_i, R_j and S$.

5.1. **BAN logic rules.** The following are the main logical postulates of the BAN logic:

- The message meaning rule:

$$\frac{P_1 \mid \equiv \ P_1 \stackrel{k}{\longleftrightarrow} P_2, P_1 \ \triangleleft \{Q_1\}_k}{P_1 \mid \equiv \ P_2 \mid \sim Q_1}$$

TABLE 4. Simulation queries

Simulation queries
If stored parameters (s, r) exist in L_H, r is returned as the result for a hash query. Otherwise, SUL selects a random value $r \in \{0,1\}^l$, answer with r, and (s, r) in L_H are selected Similar steps must be completed in the database (l, s, r) for $h_1(s)$.
$SULL$ computes the following steps for a $Send(T_i, INIT)$ query: Tag login with ID_T, PW_T and r Computes $PWT^* = h(r^* \| PW_T^* \| ID_T^*)$, $V_1^* = V_3 \oplus PWT^*$ and $V_2^* = h(V_1^* \| PWT^* \| ID_T^*)$ Verifies $V_2^* \stackrel{?}{=} V_2$ Generates random value x Computes $x' = x \oplus (V_2 \oplus s_i)$, $W_1 = h(V_3 \| ID_T \| PWT \| V_2)$ Encrypts $E_1 = E_{(V_2 \oplus V_3)}(x', W_1)$ Returns $M_1 = \{E_1, t_1\}$
For a Send (T^i, R^t, M_1) query, the following are the activities taken by SUL: Verifies $t_2 - t_1 \stackrel{?}{\leq} \triangle t$ Returns $M_2 = \{E_1, t_3\}$
For a Send (R^t, S^j, M_2) query, the actions taken by SUL are as follows Verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$ Decrypts $(x', W_1) = D_{(V_2 \oplus V_3)}(E_1)$ Computes $W_1^* = h(V_3 \| ID_T \| PWT \| V_2)$ Verifies $W_1^* \stackrel{?}{=} W_1$ Computes $x^* = x' \oplus (V_2 \oplus s_i)$ Generates random value y Computes $SK_{ST} = h(ID_T \| x^* y g \| s_i \| t_5)$, $y' = ((y \oplus W_1^*) \oplus (V_3 \oplus s_i))$, $W_2 = h(PWT \| x^* \| y \| t_5 \| V_3)$ Encrypts $E_2 = E_{((V_3 \oplus s_i) \oplus W_1^*))}(y', W_2, t_5)$ Then, answer the query with message $M_3 = \{E_2, t_5\}$ to R_j
For a Send (S^j, R^t, M_3) query, SUL performs the following actions: Verifies $t_6 - t_5 \stackrel{?}{\leq} \triangle t$ Returns $M_4 = \{E_2, t_7\}$
For a Send (R^t, T^i, M_4) query, SUL takes as below: Verifies $t_8 - t_7 \stackrel{?}{\leq} \triangle t$ Decrypts $(y', W_2, t_5 x', W_1) = D_{((V_3 \oplus s_i) \oplus W_1))}(E_2)$ Computes $y^* = ((y' \oplus W_1) \oplus (V_3 \oplus s_i))$, $W_2^* = h(PWT \| x \| y^* \| t_5 \| V_3)$ Verifies $W_2^* \stackrel{?}{=} W_2$ Computes $SK_{TS} = h(ID_T \| y^* x g \| s_i \| t_5)$
All *Send* queries are performed in order for an *Execute* (T^i, R^t, S^j) query. Massage (M_1, M_2, M_3, M_4) is the result.
If a safe session key has been provided and the probability I^K has been settled, return SK_{ST} or SK_{TS} for a *Reveal* (I^K) query. If not, the response is a $\perp$.
The response for a *Corrupt* (I^K) query is all of I^K's information.
If I^K is not $sfs - fresh$ for a $Test$ (I^K) query, $\perp$ is returned. A coin η is tossed if this is not the case. A random value of length l is returned if $\eta = 0$. If $\eta = 1$, the relevant session key is conclusion.

TABLE 5. BAN logic Notation

Notation	Description
P_1, P_2	principals
Q_1, Q_2	statements
SK	session key
$P_1 \mid\equiv Q_1$	P_1 believes Q_1
$P_1 \mid\sim Q_1$	P_1 once said Q_1
$P_1 \Rightarrow Q_1$	P_1 has got jurisdiction of Q_1
$P_1 \lhd Q_1$	P_1 receives Q_1
$\#Q_1$	Q_1 fresh
$\#\{Q_1\}_k$	Q_1 is encrypted with key k
$< Q_1 > Q_2$	X is combined with Y
$P_1 \overset{k}{\longleftrightarrow} P_2$	P_1 *and* P_2 have shared key k
T_i	RFID Tag
R_i	RFID Reader
S	Cloud database server

- The freshness rule:

$$\frac{P_1 \mid \equiv \#(Q_1)}{P_1 \mid \equiv \#(Q_1, Q_2)}$$

- The nonce-verification rule:

$$\frac{P_1 \mid\equiv \#(Q_1), P_1 \mid\equiv P_2 \mid\sim Q_1}{P_1 \mid\equiv P_2 \mid\equiv Q_1}$$

- The belief rule:

$$\frac{P_1 \mid \equiv (Q_1, Q_2)}{P_1 \mid\equiv Q_1}$$

- The jurisdiction rule:

$$\frac{P_1 \mid\equiv P_2 \mid\Rightarrow Q_1, Q_1 \mid\equiv P_2 \mid\equiv Q_1}{P_1 \mid\equiv Q_1}$$

5.1.1. *BAN logic Goals.* To assess the BAN logic proof, we present the goals of the proposed scheme as below.

- $Goal_1 : T_i \mid\equiv T_i \overset{SK}{\longleftrightarrow} R_j$
- $Goal_2 : R_j \mid\equiv T_i \overset{SK}{\longleftrightarrow} R_j$
- $Goal_3 : T_i \mid\equiv R_j \mid\equiv T_i \overset{SK}{\longleftrightarrow} R_j$
- $Goal_4 : R_j \mid\equiv T_i \mid\equiv T_i \overset{SK}{\longleftrightarrow} R_j$

5.1.2. *Idealized Forms.* To assess the BAN logic proof, we define the assumptions of the proposed scheme as below:

- Message-1 : $T_i \rightarrow R_j : M_1 = \{E_1, t_1\}_{W_1}$
- Message-2 : $R_j \rightarrow S : M_2 = \{E_1, t_3\}_{W_2}$
- Message-3 : $S \rightarrow R_j : M_3 = \{E_2, t_5\}_{W_2}$
- Message-4 : $R_j \rightarrow T_i : M_4 = \{E_2, t_7\}_{W_1}$

5.1.3. *Assumptions.* We present the initial assumptions to assess the BAN logic proof.

- $Assumption_1$: $R_j| \equiv (T_i \overset{W_1}{\longleftrightarrow} R_j)$
- $Assumption_2$: $R_j| \equiv \#(t_1)$
- $Assumption_3$: $S| \equiv (R_j \overset{W_1}{\longleftrightarrow} S)$
- $Assumption_4$: $S| \equiv \#(t_3)$
- $Assumption_5$: $R_j| \equiv (S \overset{W_2}{\longleftrightarrow} R_j)$
- $Assumption_6$: $R_j| \equiv \#(t_5)$
- $Assumption_7$: $T_i| \equiv (R_j \overset{W_2}{\longleftrightarrow} T_i)$
- $Assumption_8$: $T_i| \equiv \#(t_7)$
- $Assumption_9$: $T_i| \equiv S \Rightarrow (T_i \overset{SK}{\longleftrightarrow} S)$
- $Assumption_{10}$: $S| \equiv T_i \Rightarrow (T_i \overset{SK}{\longleftrightarrow} S)$

5.1.4. *Proof Using BAN Logic.* The proof then proceeds as below:

- Step-1: According to message-1, we could get:
$$S_1 : R_j \lhd (E_1, t_1)_{W_1}$$
- Step-2: Using the message meaning rule with $S_1 and A_1$, we get.
$$S_2 : R_j| \equiv T_i| \sim (E_1, t_1)_{W_1}$$
- Step-3: From the freshness rule with $S_2 and A_2$, we obtain
$$S_3 : R_j| \equiv \#(E_1, t_1)_{W_1}$$
- Step-4: Using the nonce verification with $S_2 and S_3$, we get
$$S_4 : R_j| \equiv T_i| \equiv (E_1, t_1)_{W_1}$$
- Step-5: From the belief rule with S_4, we obtain
$$S_5 : R_j| \equiv T_i| \equiv (E_1, t_1)_{W_1}$$
- Step-6: According to message-2, we could get:
$$S_6 : S \lhd (E_1, t_3)_{W_1}$$
- Step-7: Using the message meaning rule with $S_6 and A_3$, we get.
$$S_7 : S| \equiv R_j| \sim (E_1, t_3)_{W_1}$$
- Step-8: From the freshness rule with $S_7 and A_4$, we obtain
$$S_8 : S| \equiv \#(E_1, t_3)_{W_1}$$
- Step-9: Using the nonce verification with $S_7 and S_8$, we get
$$S_9 : S| \equiv R_j| \equiv (E_1, t_3)_{W_1}$$
- Step-10: According to message-3, we could get:
$$S_{10} : R_j \lhd (E_2, t_5)_{W_2}$$
- Step-11: Using the message meaning rule with $S_{10} and A_5$, we get.
$$S_{11} : R_j| \equiv S| \sim (E_2, t_5)_{W_2}$$
- Step-12: From the freshness rule with $S_{11} and A_6$, we obtain
$$S_{12} : R_j| \equiv \#(E_2, t_5)_{W_2}$$
- Step-13: Using the nonce verification with $S_{11} and S_{12}$, we get
$$S_{13} : R_j| \equiv S| \equiv (E_2, t_5)_{W_2}$$

- Step-14: According to message-4, we could get:
$$S_{14} : T_i \lhd (E_2, t_7)_{W_2}$$
- Step-15: Using the message meaning rule with $S_{14} and A_7$, we get.
$$S_{15} : T_i| \equiv R_j| \sim (E_2, t_7)_{W_2}$$
- Step-16: From the freshness rule with $S_{15} and A_8$, we obtain
$$S_{16} : T_i| \equiv \#(E_2, t_7)_{W_2}$$
- Step-17: Using the nonce verification with $S_{15} and S_{16}$, we get
$$S_{17} : T_i| \equiv R_j| \equiv (E_2, t_7)_{W_2}$$
- Step-18: From the belief rule with S_{17}, we obtain
$$S_{18} : T_i| \equiv R_j| \equiv T_i \overset{SK}{\longleftrightarrow} R_j \qquad (Goal - 3)$$
- Step-19: Using the jurisdiction rule with $S_{18} and A_9$, we get
$$S_{19} : T_i| \equiv T_i \overset{SK}{\longleftrightarrow} R_j \qquad (Goal - 1)$$
- Step-20: Because of SK, from the $S_5, S_9, S_{13} and S_{17}$ we could get
$$S_{20} : R_j| \equiv T_i| \equiv T_i \overset{SK}{\longleftrightarrow} R_j \qquad (Goal - 4)$$
- Step-21: Using the jurisdiction rule with $S_{19} and A_{10}$, we obtain
$$S_{21} : R_j| \equiv T_i \overset{SK}{\longleftrightarrow} R_j \qquad (Goal - 2)$$

Referring to Goals 1–4, we show that proposed scheme achieves secure mutual authentication among $T_i, R_j and S$.

5.2. **Informal security analysis.** The following is a discussion of RAVCC's informal security study:

5.2.1. ***Message authentication***. In RAVCC, R_j receives the message $M_1 = \{x', W_1, t_1\}$, $M_3 = \{W_2, y', t_5\}$, verifies $t_2 - t_1 \overset{?}{\leq} \triangle t$ and $t_6 - t_5 \overset{?}{\leq} \triangle t$. S receives $M_2 = \{x', W_1, t_3\}$, verifies $t_4 - t_3 \overset{?}{\leq} \triangle t$ and $W_1^* \overset{?}{=} W_1$. T_i receives the message $M_4 = \{M_3, t_7\}$, verifies $t_8 - t_7 \overset{?}{\leq} \triangle t$ and $W_2^* \overset{?}{=} W_2$. If verification fails, $\mathbb{A}$ will be unable to recognise any messages sent over an open channel. As a result, RAVCC achieves message authentication between T_i and S.

5.2.2. ***Mutual authentication***. In RAVCC, T_i computes $W_1 = h(V_3 \| ID_T \| PWT \| V_2)$ and sends W_1 to S via R_j. Then, S computes $W_1^* = h(V_3 \| ID_T \| PWT \| V_2)$ and verifies $W_1^* \overset{?}{=} W_1$. Further, S computes $W_2 = h(PWT \| x^* \| y \| t_5 \| V_3)$ and sends W_2 to T_i via R_j. After that, T_i computes $W_2^* = h(PWT \| x \| y^* \| t_5 \| V_3)$ and verifies $W_2^* \overset{?}{=} W_2$. Thus, both T_i and S have mutual authenticated. As a result, RAVCC is able to obtain the characteristic.

5.2.3. ***Anonymity property***. During the process of login and authentication, tag user T_i does not send his/her ID_T and PW_T to R_j and S. As a result, RAVCC endorses the anonymity attribute.

5.2.4. ***Insider attack***. In the registration phase, T_i takes ID_T, PW_t, r and calculates $PWT = h(r \| PW_T \| ID_T)$, where PW_T is the password, ID_T is the identification of the tag, and r is the random value created by T_i. So, the administrator of the is unable to got PWT. Hence, RAVCC defends against this attack.

Table 6. Costs of computation in comparison

Protocol	Total cost	Total execution time (s)
Jiant et al. [23]	$6T_{ECM} + 4T_{SYM} + 10T_H$	0.155
Sharma et al. [20]	$10T_H + 5T_{ECM} + 2T_{ECA}$	0.1016
Yan et al. [17]	$4T_{ME} + 5T_{SYM}$	0.256
Wang et al. [21]	$T_{FE} + 7T_H + 2T_{ME} + 2T_{SYM}$	0.1436
Shi et al. [24]	$15T_H + 6T_{ecm}$	0.1086
He et al. [19]	$6T_{ECM} + 2T_{ECA} + 4T_{ME} + T_{BP} + 10T_H$	0.6605
Choi et al. [40]	$16T_H + 6T_{ecm}$	0.1096
Liu et al. [22]	$4T_H + 2T_{ECM} + 1T_{BP} + 2T_{SYM}$	0.425
RAVCC	$6T_H + 4T_{ECM}$	0.0708

5.2.5. ***Replay attack***. To prevent replay attacks, the RAVCC makes use of t_i and a random nonce. The following steps are taken in login and authentication phase by T_i, R_j, and S:

- Initially, R_j verifies $t_2 - t_1 \overset{?}{\leq} \triangle t$ and $t_6 - t_5 \overset{?}{\leq} \triangle t$, where the maximum time limit is denoted by the $triangleT$.
- S checks $t_4 - t_3 \overset{?}{\leq} \triangle t$. RAVCC uses S to create a random value y.
- T_i verifies $t_8 - t_7 \overset{?}{\leq} \triangle t$. T_i select random value x and uses RAVCC.

Even if $\mathbb{A}$ replicates the eavesdropped message via the insecure channel, the session key remains elusive. As a result, RAVCC is immune to this type of attack.

5.2.6. ***Tag impersonation attack***. $\mathbb{A}$ allows you to impersonate tag in two ways: the first is to obtain PW_T and ID_T and second is by computes $M_1 = \{x', W_1, t_1\}$. For this $\mathbb{A}$ achieves $PW_{\mathbb{A}}$, $PWT_{\mathbb{A}} = h(r\|PW_{\mathbb{A}}\|ID_T^*)$, computes $V_{\mathbb{A}}^* = V_3 \oplus PWT_{\mathbb{A}}$. but $\mathbb{A}$ cannot compute $V_2^* = h(V_{PWT_{\mathbb{A}}}^*\|PWT_{\mathbb{A}}\|ID_T)$. As a result, RAVCC protects against this type of attack.

5.2.7. ***Provision of key agreement***. In RAVCC, T_i and S verify other's identities with $x^*yg = x^*yg$ and agree the session key $SK_{ST} = h(ID_T\|x^*yg\|s_i\|t_5) = SK_{TS} = h(ID_T\|x^*yg\|s_i\|t_5)$ which shows that $SK = SK_{ST} = SK_{TS}$. The random variables x and y are used to produce this session key. Using ECCDHP to execute a session key is difficult.

5.2.8. ***De-synchronization attack***. On both the server and user sides, there are no parameters that need to be modified. If a T_i wants to change the password, it can do so during the login and verification process. Furthermore, the T_i and S do not need to be synchronised for RAVCC to work. As a result, a de-synchronization assault against RAVCC's login and authentication phase will have no effect.

5.2.9. ***Parallel session attack***. This attack occurs when a $\mathbb{A}$ reprocesses earlier messages on an unprotected channel to generate a new request. In order to obtain the key, $\mathbb{A}$ impersonates the user T_i. Because the secret credentials necessary to compute content must be known by $\mathbb{A}$, user T_i can only compute a valid login request or execute the session key after that. The foregoing analysis clearly reveals that obtaining the session key with $\mathbb{A}$ is impossible. As a result, RAVCC is able to ward off this attack.

6. **Performance analysis.** We looked at a few different vehicle cloud computing techniques and compared them to RAVCC.RAVCC's computation time and communication cost were compared to other related schemes such as Yan et al.'s [17],He et al.'s [19], Wang et al.'s [21], Jiang et al.'s [23], Sharma et al.'s [20], Choi et al. [40], Shi et al. [24].

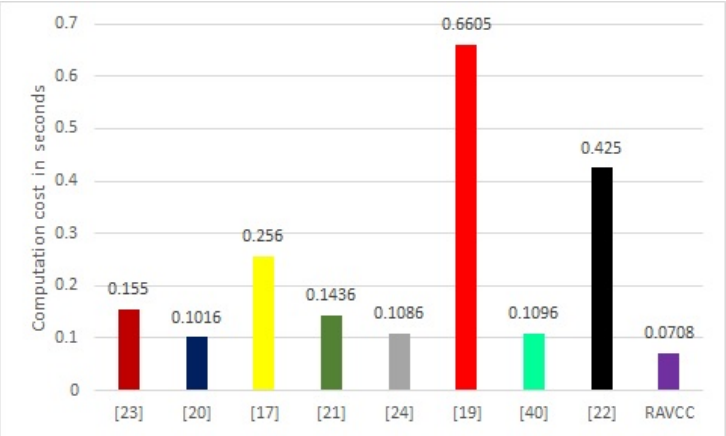

FIGURE 2. Cost of computation comparison

TABLE 7. Cost of communication comparison

Protocol	**Communication cost in bits**
Jiant et al. [23]	3104
Sharma et al. [20]	1536
Yan et al. [17]	3048
Wang et al. [21]	1188
Shi et al. [24]	3968
He et al. [19]	3296
Choi et al. [40]	3584
Liu et al. [22]	2440
RAVCC	1280

6.1. **Comparison of the computation cost.** This section compares RAVCC's computing costs to those of other existing methods like [23, 19, 17, 20, 22, 21, 24, 40]. We look at symmetric key encryption/decryption T_{SYM} and hash functions T_H as examples of cryptographic approaches. Amin et al.'s [41, 42] have used MIRACL, a C/C++ library, to compute the approximate computing time of several cryptographic techniques. The AES algorithm, " the Visual C++ 2008 S/W, the 32-bit Windows 7 OS, a 1024-bit cyclic group, a 160-bit prime field F_q, and the SHA-1 hash function " were all considered. The hash function is represented by T_H, elliptic curve multiplication is represented by T_{ECM}, bilinear pairing is represented by T_{BP}, modular exponential is represented by T_{ME}, and elliptic curve addition is represented by T_{ECA}. The SHA-1 and AES routines' approximate computing times are recorded as "$T_H \approx 0.0004$ s, $T_{ECM} \approx 0.0171$ s" and is time of an EC scalar multiplication respectively and $T_{SYM} \approx 0.0056$s, $T_{ECA} \approx 0.0061s$, $T_{BP} \approx 0.314s$, $T_{ME} \approx 0.057$ It is commonly known that concatenation ($\|$) and XOR ($\oplus$) operations have very low processing costs. The total $4T_{ECM} + 6T_H$ operations are executed in RAVCC as a full computation. The computation cost of RAVCC and comparable protocols [23, 19, 17, 20, 22, 21, 24, 40] that are already in use in the environment are shown in the table 6. In comparison to the relevant current protocols, the RAVCC is more secure. In addition, Figure 2 shows the cost of computation comparison.

6.2. **Comparison of the communication cost.** To compare transmission costs, we divide "the length of the time-stamp, random number, password, and identity into 64 bits each. The message digest of the hash function (SHA-1) will be 160 bits, symmetric

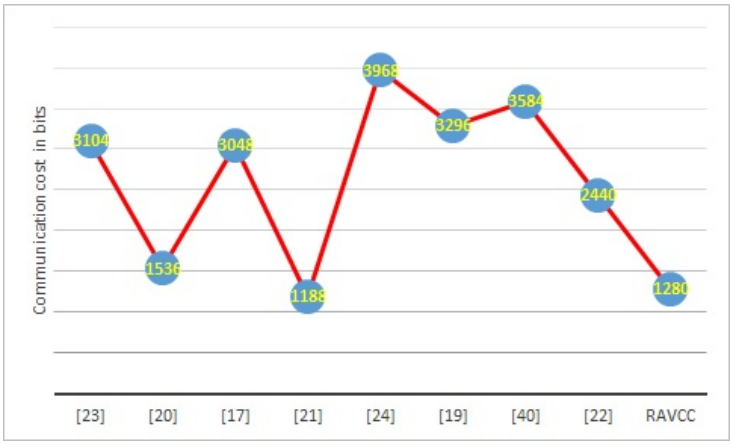

FIGURE 3. Cost of communication comparison

key encryption/decryption (AES-256) will be 256 bits, and ECC scalar multiplication will be 160 bits [41, 43, 42]". RAVCC's performance was evaluated and compared to a comparable scheme in a communication setting. RAVCC's communication cost is 1280 bits. In comparison to the other protocols, RAVCC appears to be more secure. In Table 7, you can see a comparison of communication costs. The details of the communication cost comparison are also shown in Figure 3.

7. **Conclusion.** RFID-based structures are a must-have method in today's networking world. It is in charge of the evolution of the communication system. Its features include minimal cost and the ability to identify systems automatically. Due to the fact that RFID technology uses small and low radio frequencies, it has security, counterfeiting, and privacy difficulties in network connection. For VCC, we have recommended an authentication architecture based on elliptic curve encryption and an RFID. To demonstrate that the proposed approach ensures secure communication, we have used formal security analysis in the random oracle model, Ban logic and informal security analysis. We have compared the proposed framework to similar systems and tested its performance against desirable performance parameters. According to our findings, the proposed architecture meets all security requirements while also allowing for effective communication.

References

[1] S. Olariu, I. Khalil, and M. Abuelela, "Taking vanet to the clouds," *International Journal of Pervasive Computing and Communications,* vol. 7, no. 1, pp. 7–21, 2011.

[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems,* vol. 50, no. 4, pp. 217–241, 2012.

[3] N. Tekbiyik and E. Uysal-Biyikoglu, "Energy efficient wireless unicast routing alternatives for machine-to-machine networks," *Journal of Network and Computer Applications,*vol. 34, no. 5, pp. 1587–161, 2011.

[4] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *Journal of Network and Computer Applications,* vol. 34, no. 4, pp. 1138–1149, 2011.

[5] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications,* vol. 40, pp. 325–344, 2014.

[6] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications,* vol. 75, pp. 200–222, 2016.

[7] S. Ting, S. K. Kwok, A. H. Tsang, and W. Lee, "Critical elements and lessons learnt from the implementation of an rfid-enabled healthcare management system in a medical organization," *Journal of medical systems,* vol. 35, no. 4, pp. 657–669, 2011.

[8] S. F. Wamba, A. Anand, and L. Carter, "A literature review of rfid-enabled healthcare applications and issues," *International Journal of Information Management,* vol. 33, no. 5, pp. 875–891, 2013.
[9] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and privacy in rfid and applications in telemedicine," *IEEE communications magazine,* , vol. 44, no. 4, pp. 64–72, 2006.
[10] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-based security processor for rfid," *IEEE Transactions on Computers,* vol. 57, no. 11, pp. 1514–1527, 2008.
[11] A. Kumari, M. Yahya Abbasi, V. Kumar, and A. A. Khan, "A secure user authentication protocol using elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography,* , vol. vol 22, no. 4, pp. 521–530, 2019.
[12] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. Mittal, "A hash based mutual rfid tag authentication protocol in telecare medicine information system," *Journal of medical systems,* vol. 39, no. 1, pp. 153, 2015.
[13] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "A secure rfid tag authentication protocol with privacy preserving in telecare medicine information system," *Journal of medical systems,* vol. 39, no. 8, pp. 77, 2015.
[14] H. Ning, H. Liu, J. Mao, and Y. Zhang, "Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems," *IET communications,* vol. 5, no. 12, pp. 1755–1768, 2011.
[15] Y. Chen and J.-S. Chou, "Ecc-based untraceable authentication for large-scale active-tag rfid systems," *Electronic Commerce Research,* vol. vol. 15, no. 1, pp. 97–120, 2015.
[16] A. Kumari, V. Kumar, M. YahyaAbbasi, and M. Alam, "The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for iot and cloud servers," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 321–325, 2018.
[17] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems*, pp. 370–375, 2012.
[18] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE systems journal*vol. 9, no. 3, pp. 805–815, 2015.
[19] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Systems Journal,* vol. 12, no. 2, pp. 1621–1631, 2016.
[20] M. K. Sharma, R. S. Bali, and A. Kaur, "Dyanimc key based authentication scheme for vehicular cloud computing," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1059–1064, 2015.
[21] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 2, pp. 896–911, 2015.
[22] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems,* vol. 18, pp. 10, pp. 2740–2749, 2017.
[23] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," *IEEE Network,* vol. 32, no. 3, pp. 28–35, 2018.
[24] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks,* vol. 9, no. 4, pp. 730831, 2013.
[25] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors,*vol. 14, no. 6, pp. 10081–10106, 2014.
[26] M. A. Pandi Vijayakumar, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. vol,17, no. 4, 2016.
[27] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent rfid-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications,* vol. 9, no. 5, pp. 824–840, 2016.
[28] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, and J. Shen, "A lightweight and anonymous rfid tag authentication protocol with cloud assistance for e-healthcare applications," *Journal of Ambient Intelligence and Humanized Computing,* vol. 9, no. 4, pp. 919–930, 2018.
[29] N. Dinarvand and H. Barati, "An efficient and secure rfid authentication protocol using elliptic curve cryptography," *Wireless Networks,* vol. 25, no. 1, pp. 415–428, 2019.

[30] V. Kumar, M. Ahmad, and P. Kumar, "An identity-based authentication framework for big data security," in *Proceedings of 2nd International Conference on Communication, Computing and Networking*, pp. 63–71, 2019.

[31] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "Rseap: Rfid based secure and efficient authentication protocol for vehicular cloud computing," *Vehicular Communications,* vol. 22, pp. 100213, 2020.

[32] Y.-C. Chen, H.-M. Sun, and R.-S. Chen, "Design and implementation of wearable rfid tag for real-time ubiquitous medical care," in *Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS), 2014 IEEE Topical Conference on* , pp. 25–27, 2014.

[33] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "Rfid technology for iot-based personal healthcare in smart spaces," *IEEE Internet of things journal,* vol. 1, no. 2, pp. 144–152, 2014.

[34] N. F. B. I. Gulcharan, H. Daud, N. M. Nor, T. Ibrahim, and E. T. Nyamasvisva, "Limitation and solution for healthcare network using rfid technology: a review," *Procedia Technology*vol. 11, pp. 565–571, 2013.

[35] M. Abdalla, M. Izabachene, and D. Pointcheval, "Anonymous and transparent gateway-based password-authenticated key exchange," in *International Conference on Cryptology and Network Security*, pp. 133–148, 2018.

[36] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *Journal of medical systems,* vol. 36, no. 6, pp. 3833–3838, 2012.

[37] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to-Peer Networking and Applications,* vol. vol 10, no. 1, pp. 16–30, 2017.

[38] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. Khan, "Sebap: A secure and efficient biometric-assisted authentication protocol using ecc for vehicular cloud computing," *International Journal of Communication Systems,*, pp. e4103, https://doi.org/10.1002/dac.4103, 2019.

[39] V. Kumar, M. S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, and A. Kumari, "Rapchi: Robust authentication protocol for iomt-based cloud-healthcare infrastructure," *The Journal of Supercomputing*, pp. pp. 1–30, 2022.

[40] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors,* vol. 14, no. 6, pp. 10081–10106, 2014.

[41] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems,* vol. 80, pp. 483–495, 2018.

[42] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ecc," *Computer Communications,* vol. 110, pp. 26–34, 2017.

[43] R. Amin and G. Biswas, "A secure three-factor user authentication and key agreement protocol for tmis with user anonymity," *Journal of medical systems,* vol. 39, no. 8, 2015.