Construction of Authentication Scheme using ECC for Vehicular Cloud Computing

Kamal Kumar
Department of Mathematics
Baba MastnathUniversity
Rohtak-124021, India

Vinod Kumar
Department of Mathematics
Shyam Lal College, University of Delhi
New Delhi-110032, India

Renu
Department of Mathematics
Baba MastnathUniversity
Rohtak-124021, India

Adesh Kumari
Department of Mathematics
Jamia Millia Islamia
New Delhi-110025, India

Rajiv Sharma
Department of Computer Science and Engineering
Baba MastnathUniversity
Rohtak-124021, India

ABSTRACT

Vehicular cloud computing (VCC) is a combination of cloud computing, Internet of Things (IoT), vehicular networking, and other technologies. The term VCC Communication refers to the communication between automobiles that have communication sensing capabilities. This includes vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-device (V2D) interactions. Cloud computing, IoTs, and vehicle resources are all utilized by VCC. However, VCC highlights how crucial communication security and privacy are for communicators. We offer an ECC based authentication framework for VCC, which is equipped with vehicle user and cloud server, with the goal of enabling safe communication while maintaining anonymity. We use security analysis as evidence for the safe communication assertion. We justify and assess the recommended framework's performance in terms of acceptable performance metrics and draw comparisons with other systems of a like nature. Based on our findings, the suggested architecture allows for efficient communication while meeting the necessary security requirements.

Keywords

ECC, Authentication, Vehicular cloud computing, Security and Privacy

1. INTRODUCTION

Thanks to developments in transmission infrastructure, software, and hardware, the researchers were able to examine and evaluate a large variety of network applications under various conditions. The Vehicular Ad-Hoc Network (VANET) [1, 2] has drawn a lot of attention lately as a novel paradigm for information transfer in a conventional automobile network. The objectives of VCC are to cut travel times, prevent accidents, and ease traffic congestion by giving cars with low computer power real-time computing capabilities. adoption of the technology will thereby benefit the environment. Furthermore, for improved road safety and an informed urban transportation system, VCC theoretically enables the integration of " Wireless Sensor Networks, Mobile Cloud Computing, and Intelligent Transportation Systems" [3].

In the context of V2V communication, network connections from V2I or V2V link each vehicle to the network communication infrastructures [4]. Some of the cloud services that the VCC uses are "platform as a service, entertainment as a service, infrastructure as a service, function as a service, data as a service, pictures on a wheel as a service, computing as a service, information as a service, storage as a service, network as a service, collaboration as a service, and so on". Using user feedback based on historical data, this application can be used for a multitude of tasks, including obtaining information about neighboring base stations and roadside units, gathering traffic data, sending emergency message/call alerts, managing staff availability, and maintaining an intelligent and skilled environment. In this context, the cloud facilitates the collection, processing, and management of user data. The real-world security problems of the client are believed to originate from the base stations of the roadside unit, which are in sync with the cloud [5].

The goal of VCC is to improve vehicle networking and functioning by providing a wide range of cloud services. Pictures on a Wheel as a Service, Computing as a Service (CaaS), Platform as a Service (PaaS), Data as a Service (DaaS), Function as a Service (FaaS), Entertainment as a Service (EaaS), Storage as a Service (SaaS), Network as a Service (NaaS), and Collaboration as a Service (CaaS) are some of these services. For vehicles to operate well and remain connected within the VCC ecosystem, each of these services is essential. In order to connect cars to the larger network infrastructure, the VCC communication area is principally enabled by PaaS. Every vehicle can link to other vehicles or network communication infrastructures thanks to this domain's support for both V2I and V2V communication. The ability for vehicles to communicate and coordinate data in real-time is critical for optimizing traffic management, boosting security, and offering cutting-edge vehicular services [6]. VCC utilizes a variety of cloud-based technologies, including Development as a Service (DaaS), Mobile Backend as a Service, Infrastructure as a Service (IaaS), and Information as a Service. All of these services work together to fulfill the VCC's needs, which range from processing and storing data to developing and implementing applications. Mobile Backend as a Service, for example, makes sure that mobile applications can effectively communicate with backend systems, while architecture as a Service (IaaS) offers the architecture required to enable scalable and flexible computing resources. It is possible to create a reliable and flexible system that can satisfy the changing needs of contemporary vehicle networks by integrating these various cloud services into the VCC model. VCC makes sure that every car can connect to the network and contribute in an efficient manner by using PaaS for its communication domain. This leads to better collaboration and data exchange. In addition to improving each vehicle's performance and usefulness, this all-encompassing strategy advances intelligent transportation systems as a whole [4].

1.1 Related work

This section of the study provides an overview of the literature review that supports the recommended procedure. Yan et al. mentioned a security risk with automobile cloud computing [7]. To get around certain fundamental issues, they developed a VCC architecture that offers privacy and security in the car. This study addressed VCC's security concerns for the first time. For efficient and private mobile-based cloud computing, Tsai and Lo [8] presented an authentication method. They said that the recommended method authenticates the user as well as the service provider and is safe and secure. Liu et al. were able to reduce the communication overhead and withdraw user functionality using the suggested method. Nonetheless, the overall computation time of the strategy did not drop as much as they claimed. A significant agreement protocol was put forth by Liu et al. for the internet of vehicles [9]. For vehicle-to-vehicle authenticated communication, Liu et al. claim that the proposed method works well. Also, there has been an improvement in the security of car network connectivity. A non-interactive key agreement method was developed for automotive cloud computing by Jiang et al. [10]. The suggested method uses a cloud environment, with identity as its foundation, and includes vehicle authentication. In order to accomplish this, though, more communication overhead is needed. An ECC-based user authentication system that is resistant to " parallel session attacks, off-line password guessing assaults, anonymity and untraceable attacks" was proposed by Shi et al. for wireless sensor networks (WSNs) [11]. A safe authentication system based on the ECC work was developed by Choi et al. [12] for WSNs; it excludes the usage of password changing phases, anonymity, mutual authentication, impersonation, and untraceable attacks. A safe and efficient vehicle ad-hoc communications system was proposed by Vijayakumar et al. [13].

1.2 Motivation and contribution

It is acknowledged that several authentication methods for VCC systems have been established over the last few decades [14, 15, 16, 17, 18, 19], drawing from the existing corpus of literature. For VCC systems, however, there are no verified key agreement procedures. Carrier users and VCCs demand distinct processing power and privacy requirements, which makes authenticated key agreements essential in aided VCC systems. We address this by offering an authenticated key agreement approach for VCC systems that is based on ECC. The following are some noteworthy features of the proposed plan:

- The procedure of authentication supports the key that is created between the vehicle user and the VC database server.
- The security of the strategy is shown appropriately.
- A shared session key is calculated and agreed upon by the cloud server and the vehicle user.
- The suggested protocol offers desired performance characteristics, according to the comparative results and performance analysis.

1.2.1 ***Organization of the paper***. The rest of the paper's layout is as follows: Section 2 contains the system model and preliminary data. The suggested protocol is covered in Section 3. Section 4 of the proposed protocol contains a security investigation. Section 5 discusses the effectiveness of the recommended protocol. We will now discuss the conclusion. Notations from Table 1 are also utilized.

2. PRELIMINARIES AND SYSTEM MODEL

2.1 The principles of ECC within a finite field

Let $E_q(a,b) : y^2 = x^3 + ax + b \bmod q$, be a non singular elliptic curve over a finite field $Z_q^\star$ where $a, b \in Z_q^\star$ with $4a^3 + 27b^2 \bmod q \neq 0$ and $G = \{(x,y) : x, y \in Z_q, (x,y) \in E\} \cup \{\theta\}$, according to [15], θ represents group identity under addition. Several operations can be carried out on G [20], including the following ones:

1. Let $X = (x,y) \in G$, then define $-X = (x,-y)$ and $X + (-X) = \theta$
2. Let $X = (x,y) \in G$ then the scalar multiplication is defined as: $nX = X + X + X................ + X\ (n - times)$.
3. If $X = (x_1, y_1), Y = (x_2, y_2)$, then $X + Y = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - y_2\ mod\ q$ and $y_3 = \lambda(x_1 - x_2) - y_1\ mod\ q$, with

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}\ mod\ \text{q}\ if\ \ X\ \neq Y \\ \\ \frac{3x_1^2 + b}{2v_1}\ mod\ \text{q}\ if\ \ X\ = Y \end{cases}$$

—**Elliptic curve discrete logarithm problem (ECDLP)**: For inputs $X, Y \in G$, computationally hard to calculate $t \in Z_q^*$ such that $X = tY$ [21].

—**Elliptic curve computational Diffie-Hellman problem (EC-CDHP)**: Let $x, y \in Z_q^*$ and g is generator of G. For input (g, ag, bg), it is computationally hard to execute abg in G [15].

2.2 Network model

The framework that is being presented is a novel approach meant to enhance the security and privacy of users of roads and roadside infrastructure. Additionally, it offers developing services and the requisite skills to clients that are moving. The suggested paradigm is based on the network system's advantages. The projected work's architecture is depicted in figure 1.

2.3 Attack model and assumptions

The attack model is displayed in respect to our recommended protocol as follows:

- By exploiting an unsecured channel, an attacker $\mathbb{A}$ might attempt to disrupt communication between vehicular user and cloud database server.

Table 1.
Notations

Symbol	Description	Symbol	Description
V_i, & S	i^{th} Vehicular user & VC server	PW_V	Password of i^{th} vehicular user
$\mathbb{A}$	Adversary	s	Secret key of S
$\mathcal{E}(F_q)$	The elliptic curve $\mathcal{E}$ over 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	$\oplus$	Bitwise XOR operation
ID_i	The i^{th} participant's identity	$\|$	Concatenation operation
G	ECC based additive group	g	Base point of G
$h(\cdot)$	Cryptographic one way hash function	Z_q^*	Group with order $q-1$ under multiplication
$SK_{ij}(.)$	A session key is shared by entities i and j.	$u \stackrel{?}{=} v$	Whether u and v are equal
VCC	The vehicular cloud computing	s_i	Serial number of i^{th} vehicle user

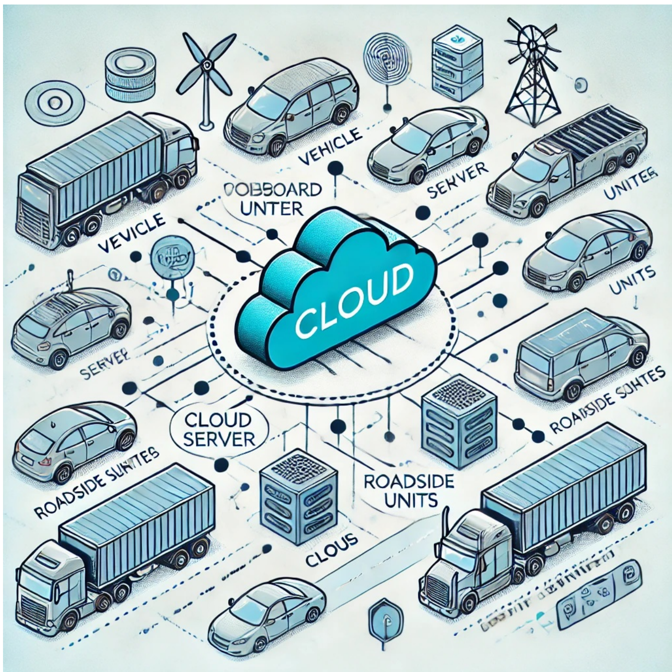

Fig. 1. The suggested protocol's architecture

- $\mathbb{A}$ may choose to utilize active attack, passive attack, or a combination of the two to deal with the vehicle user.
- Using rogue user in the structures, $\mathbb{A}$ can spoof/masquerade as the appropriate readers and tags as part of the aggression process.

For the suggested framework, we assume the following fundamentals:

- Users that travel on roads or highways wear vehicle user waistlines that are connected to the area network.
- Communication between the database server and the vehicle user needs to be safeguarded because it appears to be open.

2.3.1 ***Working methodology***. Data is transmitted to the cloud server during the authentication procedure. The VCC system uses an unprotected channel to transport data. It is possible to employ wired or wireless networks as a communication medium [15, 22].

3. THE PROPOSED PROTOCOL

3.1 Initialization phase

First, using the equation $y^2 = x^3 + ax + b$ over $Z_q^\star$, S selects EC. G generator g is selected by S from a non-singular elliptic curve. Moreover, S is defined as a secret key and yields $s \in F_q$.

3.2 Registration phase

Step RP1 After generating a random value r and executing $PWV = h(r\|PW_V\|ID_V)$, V_i registers with S by receiving ID_V, PW_V. It then sends $M_1^R = \{PWV, ID_V\}$ to S across a secure channel.

Step RP2 Creates a random serial number s_i upon receiving M_1^R. Additionally, with s serving as the secret key for S, S computes $HR_1 = h(s\|s_i\|ID_V)$, $HR_2 = h(HR_1\|PWV\|ID_V)$, and $HR_3 = HR_1 \oplus PWV$. Afterwards, S uses a secure channel to deliver $M_2^R = \{HHR_2, G, h(.), HR_3, s_i, g\}$ to T.

Step RP3 Parameters $\{HR_2, G, h(.), HR_3, s_i, g\}$ are stored in V_i's database upon receiving M_2^R.

Table 2 shows the procedure used in the registration process.

3.3 Login and authentication phase

Following a successful registration with S, V_i requests access from S in order to utilize the service. An explanation of the process is provided below:

Step LA1: V_i login using r^*, PW$_V^*$, and ID_v^*. carries out $PWV^* = h(r^*\|PW_V^*\|ID_V^*) further.Wehave V_1^* = HR_3 \oplus PWV^*$. The calculation of $HR_2^* = h(HR_1^*\|PWV^*\|ID_V^*)$ confirms that $HR_2^* \stackrel{?}{=} HR_2$. Next, a random value x is generated. Then, $W_1 = h(HR_3\|ID_V\|PWV\|HR_2)$ and $x' = x \oplus (HR_2 \oplus s_i)$ are processed.To encrypt $E_1 = E_{(HR_2 \oplus HR_3)}(x', W_1)$, use and uses the public channel to deliver $M_1 = \{E_1, t_1\}$ to S.

Step LA2 : S verifies that $t_2 - t_1 \stackrel{?}{\leq} \triangle t$ after receiving M_1. Furthermore, S works out $W_1^* = h(HR_3\|ID_V\|PWV\|HR_2)$, cracks $(x', W_1) = D_{(HR_2 \oplus HR_3)}(E_1)$, and verifies that $W_1^* \stackrel{?}{=} W_1$. Next, S computes $x^* = x' \oplus (HR_2 \oplus s_i)$, producing a random value y and computes $SK_{SV} = h(ID_V\|x^*yg\|s_i\|t_3)$, $y' = ((y \oplus W_1^*) \oplus (HR_3 \oplus s_i)), W_2 = h(PWV\|x^*\|y\|t_3\|HR_3)$, After encrypting $E_2 = E_{((HR_3 \oplus s_i) \oplus W_1^*)}$. S sends $M_2 = \{E_2, t_3\}$ to V_i via public channel.

Step LA3: V_i confirms $t_4 - t_3 \stackrel{?}{\leq} \triangle t$ after obtaining M_2. Subsequently, V_i decodes $(y', W_2, t_3, \ x', W_1) = D_{((HR_3 \oplus s_i) \oplus W_1))}(E_2)$, and calculates $y^* = ((y' \oplus W_1) \oplus$

Table 2.

Vehicle user registration

V_i	S
Inputs ID_V and PW_V a random value r is generated Computes $PWV = h(r\|PW_V\|ID_V)$ Sends $M_1^R = \{PWV, ID_V\}$ $\cdots\cdots\cdots\Rightarrow$	
	The random serial number s_i is generated. Computes $HR_1 = h(s\|s_i\|ID_V)$, where s is secret key of S Computes $HR_2 = h(HR_1\|PWV\|ID_V)$ Computes $HR_3 = HR_1 \oplus PWV$ Sends $M_2^R = \{HR_2, G, h(.), HR_3, s_i, g\}$ $\Leftarrow\cdots\cdots\cdots$
Store $\{HR_2, G, h(.), HR_3, s_i, g\}$ in database	

Table 3.

Login and authentication phase via public channel

V_i	S
Login with ID_V^*, PW_V^* and r^* Computes $PWV^* = h(r^*\|PW_V^*\|ID_V^*)$ Computes $HR_1^* = HR_3 \oplus PWV^*$ Computes $HR_2^* = h(HR_1^*\|PWV^*\|ID_V^*)$ Verifies $HR_2^* \stackrel{?}{=} HR_2$ Produces a random value of x. Computes $x' = x \oplus (HR_2 \oplus s_i)$ Computes $W_1 = h(HR_3\|ID_V\|PWV\|HR_2)$ Encrypts $E_1 = E_{(HR_2 \oplus HR_3)}(x', W_1)$ Sends $M_1 = \{E_1, t_1\}$ $\cdots\cdots\cdots\longrightarrow$	
	Verifies $t_2 - t_1 \stackrel{?}{\leq} \triangle t$ Decrypts $(x', W_1) = D_{(HR_2 \oplus HR_3)}(E_1)$ Computes $W_1^* = h(HR_3\|ID_V\|PWV\|HR_2)$ Verifies $W_1^* \stackrel{?}{=} W_1$ Computes $x^* = x' \oplus (HR_2 \oplus s_i)$ produces a random value of y Computes $SK_{SV} = h(ID_V\|x^*yg\|s_i\|t_3)$ Computes $y' = ((y \oplus W_1^*) \oplus (HR_3 \oplus s_i))$ Computes $W_2 = h(PWV\|x^*\|y\|t_5\|HR_3)$ Encrypts $E_2 = E_{((HR_3 \oplus s_i) \oplus W_1^*))}(y', W_2, t_3)$ Sends $M_3 = \{E_2, t_3\}$ $\longleftarrow\cdots\cdots\cdots$
Verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$ Decrypts $(y', W_2, t_3x', W_1) = D_{((HR_3 \oplus s_i) \oplus W_1))}(E_2)$ Computes $y^* = ((y' \oplus W_1) \oplus (HR_3 \oplus s_i))$ Computes $W_2 = h(PWV\|x\|y^*\|t_3\|HR_3)$ Verifies $W_2^* \stackrel{?}{=} W_2$ Computes $SK_{VS} = h(ID_V\|y^*xg\|s_i\|t_3)$	

$(HR_3 \oplus s_i))$.then $W_2^* = h(PWV\|x\|y^*\|t_3\|HR_3)$, and confirms that $W_2^* \stackrel{?}{=} W_2$. Set the session key as follows: $SK_{VS} = h(ID_V\|y^*xg\|s_i\|t_3)$.

This establishes mutual authentication and results in an agreed-upon session key $SK = SK_V = SK_S$ between V_i and S. Table 3 displays the process login and authentication.

4. SECURITY ANALYSIS

The security study of the suggested protocols is discussed below:

4.1 Mutual authentication

The proposed framework has V_i compute $W_1 = h(HR_3\|ID_V\|PWV\|HR_2)$, and then S receives W_1. After computing $W_1^* = h(HR_3\|ID_V\|PWV\|HR_2)$, S confirms that $W_1^* \stackrel{?}{=} W_1$. Additionally, S transfers W_2 to V_i after computing $W_2 = h(PWV\|x^*\|y\|t_3\|HR_3)$. Once $W_2^* = h(PWV\|x\|y^*\|t_3\|HR_3)$ is computed, V_i confirms that $W_2^* \stackrel{?}{=} W_2$. As a result, both V_i and S have experienced mutual authentication. Thus, the proposed protocol can get the feature.

4.2 Message authentication

According to the suggested protocol, S receives the message $M_1 = \{W_1, t_1\}$, and confirms that $W_1^* \stackrel{?}{=} W_1$ and $t_2 - t_1 \stackrel{?}{\leq} \triangle t$. When $M_2 = \{E_2, t_3\}$ is sent to V_i, it verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$ and $W_2^* \stackrel{?}{=} W_2$. In the event that verification fails, $\mathbb{A}$ will not be able to recognize any messages sent over an open channel. Using this proposed method, V_i and S can authenticate messages.

4.3 Anonymity property

Vehicle user V_i does not convey ID_V and PW_V to S during the login and authentication process. Hence, the anonymity property is supported by the suggested protocol.

4.4 Insider attack

To compute $PWV = h(r\|PW_V\|ID_V)$ during the registration phase, V_i needs ID_V, PW_V, r. In this calculation, PW_V represents the password, ID_V denotes V_i's identification, and r represents the random value that V_i generates. In light of this, the administrator of the cannot obtain PWV. For this reason, the suggested protocol counters this assault.

4.5 Replay attack

The suggested protocol uses V_i and a random nonce to thwart replay attacks. V_i, and S do the following actions throughout the login and authentication phase:

- S checks $t_2 - t_1 \stackrel{?}{\leq} \triangle t$. In the proposed protocol S create a random value y and uses in this session.
- V_i verifies $t_4 - t_3 \stackrel{?}{\leq} \triangle t$. V_i select random value x and uses in this session.

The session key is still elusive even in the event that $\mathbb{A}$ copies the message that was intercepted through the unsecure channel. The suggested protocol is therefore impervious to this kind of attack.

4.5.1 ***User impersonation attack.*** One of the two ways you can utilize $\mathbb{A}$ to play the role of the user is to compute $M_1 = \{x', W_1, t_1\}$; the other approach is to obtain PW_V and ID_V. With $\mathbb{A}$, $PW_{\mathbb{A}}$, $PWV_{\mathbb{A}} = h(r\|PW_{\mathbb{A}}\|ID_V^*)$, and $HR_{\mathbb{A}}^* = HR_3 \oplus PWV_{\mathbb{A}}$ are the results of this. Unfortunately, $\mathbb{A}$ cannot compute $HR_2^* = h(V_{PWV_{\mathbb{A}}}^*\|PWV_{\mathbb{A}}\|ID_V)$. Consequently, the recommended protocol stops this form of attack.

4.6 Key agreement provision

V_i and S verify each other's identities in the proposed protocol by using $x^*yg = x^*yg$. The session key, $SK_{SV} = h(ID_V\|x^*yg\|s_i\|t_3) = SK_{VS} = h(ID_V\|x^*yg\|s_i\|t_3)$, is also agreed upon by them, proving that $SK = SK_{SV} = SK_{VS}$. Using the random variables x and y, this session key is created. ECCDHP presents a difficulty when executing a session key.

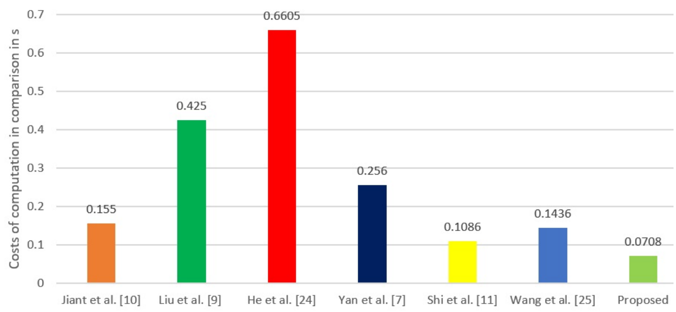

Fig. 2. Computation cost comparison

4.7 De-synchronization attack

There are no parameters that require changing on either the server or user end. During the login and verification procedure, a V_i has the option to modify its password. Moreover, the suggested protocol can function without the V_i and S being synchronized. Consequently, there will be no impact from a de-synchronization attack on the login and authentication phase of the proposed protocol.

4.7.1 ***Parallel session attack.*** On an unsecured channel, this attack happens when a $\mathbb{A}$ reprocesses previous messages to create a new request. $\mathbb{A}$ assumes the identity of user V_i in order to obtain the key. After that, user V_i can only compute a valid login request or execute the session key since $\mathbb{A}$ has to know the secret credentials required to compute content. By using $\mathbb{A}$, it is evident from the analysis above that it is impossible to retrieve the session key. Thus, this attack can be repelled by the suggested procedure.

5. PERFORMANCE ANALYSIS

We examined several distinct methods for cloud computing in cars and contrasted them with the suggested protocol. The computation time and communication cost of the proposed protocol were compared to those of other relevant schemes, including Yan et al.'s [7],He et al.'s [23], Wang et al.'s [24], Jiang et al.'s [10], Shi et al. [11].

5.1 Comparison of the computation cost

In this part, the computing costs of the proposed protocol are compared with those of other current techniques, such as [10, 23, 7, 9, 24, 11]. Symmetric key encryption/decryption T_{SYM} and hash functions T_H are examined as cryptographic techniques. Several encryption algorithms' approximate computing times have been calculated using the C/C++ package MIRACL by Amin et al. [25, 26]. The SHA-1 hash function, a 1024-bit cyclic group, a 160-bit prime field F_q, the 32-bit Windows 7 OS, the AES method, and the Visual C++ 2008 S/W were all taken into consideration. Modular exponential is represented by T_{ME}, elliptic curve addition by T_{ECA}, bilinear pairing by T_{BP}, elliptic curve multiplication by T_{ECM}, and the hash function by T_H. The approximate computation times for the SHA-1 and AES routines are $T_H \approx 0.0004$ s, $T_{ECM} \approx 0.0171$ s and is the time of an EC scalar multiplication, respectively, and $T_{SYM} \approx 0.0056$s, $T_{ECA} \approx 0.0061s$, $T_{BP} \approx 0.314s$, $T_{ME} \approx 0.057$. Most people are aware of the extremely cheap processing costs associated with the concatenation ($\|$) and XOR ($\oplus$) operations. The suggested approach performs a full computation of $4T_{ECM} + 6T_H$ operations in total. The table

Table 4.

Costs of computation in comparison

Protocol	Total computation cost	Total execution time (s)
Jiant et al. [10]	$6T_{ECM} + 4T_{SYM} + 10T_H$	0.155
Liu et al. [9]	$4T_H + 2T_{ECM} + 1T_{BP} + 2T_{SYM}$	0.425
He et al. [23]	$6T_{ECM} + 2T_{ECA} + 4T_{ME} + T_{BP} + 10T_H$	0.6605
Yan et al. [7]	$4T_{ME} + 5T_{SYM}$	0.256
Shi et al. [11]	$15T_H + 6T_{ecm}$	0.1086
Wang et al. [24]	$T_{FE} + 7T_H + 2T_{ME} + 2T_{SYM}$	0.1436
Proposed	$6T_H + 4T_{ECM}$	0.0708

4 displays the computation cost of the suggested protocol as well as similar protocols that are currently in use in the environment. The fig 2 shows the details of the computation cost.

Table 5.

Cost of communication comparison

Protocol	Communication cost in bits
Jiant et al. [10]	3104
Liu et al. [9]	2440
Yan et al. [7]	3048
Shi et al. [11]	3968
He et al. [23]	3296
Wang et al. [24]	1188
Proposed	1280

5.2 Comparison of the communication cost

The time-stamp, password, identity, and random number are all divided into 64 bits each in order to compare transmission costs. AES-256, a symmetric key encryption and decryption algorithm, has a message digest of 160 bits, while ECC scalar multiplication has a message digest of 160 bits [25, 27, 26]. Performance analysis and comparison with a similar scheme in a communication scenario were conducted for the suggested protocol. A communication cost of 1280 bits is associated with the proposed protocol. It seems that the suggested protocol is more secure than the other protocols. A comparative analysis of communication costs is presented in Table 5. The fig 3 shows the details of the computation cost.

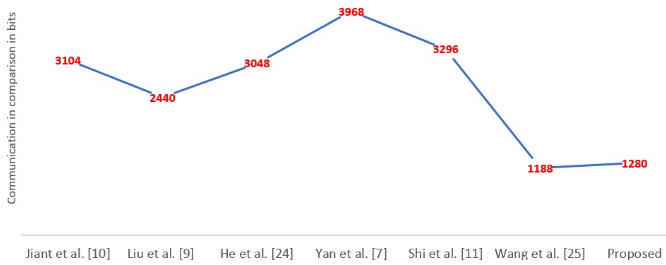

Fig. 3. Communication cost comparison

6. CONCLUSION AND FUTURE SCOPE

The work that is being offered offers a strong, practical way to improve security in intelligent transportation systems. ECC is the best option for resource-constrained contexts like VCC, where cars have limited computing power and energy resources. It offers high-level security with less computational overhead than other cryptographic techniques. The suggested authentication method guards against potential threats including man-in-the-middle, impersonation, and replay attacks while guaranteeing data integrity, confidentiality, and privacy. The technique ensures secure communication between automobiles, roadside units (RSUs), and cloud servers by utilizing ECC to achieve lightweight yet strong authentication. Additional important issues for VCC contexts that the proposed system solves are scalability to support millions of vehicles, handling dynamic and decentralized topologies, and quick authentication for time-sensitive vehicular communications. The authentication scheme's use of ECC results in a reduction of computational time and bandwidth usage while upholding a high degree of security. This efficiency is felt in the key creation, encryption, and verification procedures.

Future study and development in this field have a number of options. First, investigating how to combine ECC-based authentication with cutting-edge technologies like Blockchain will improve security and trust management even further in VCC networks. Blockchain technology offers tamper-proof logs of transactions between cars, RSUs, and cloud services, thereby decentralizing authentication procedures. Furthermore, combining 5G technology with ECC-based authentication can provide ultra-reliable and low-latency communication for real-time vehicular applications once 5G networks are widely deployed. By creating post-quantum cryptographic protocols that guarantee security in upcoming vehicle cloud networks, future research may also concentrate on overcoming the difficulties posed by quantum computing. Finally, as secure authentication mechanisms continue to be developed, increasing energy efficiency and cutting down on computation time for large-scale VCC deployments will be crucial.

7. REFERENCES

[1] S. Olariu, I. Khalil, M. Abuelela, Taking vanet to the clouds, International Journal of Pervasive Computing and Communications 7 (1) (2011) 7–21.

[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (vanets): status, results, and challenges, Telecommunication Systems 50 (4) (2012) 217–241.

[3] N. Tekbiyik, E. Uysal-Biyikoglu, Energy efficient wireless unicast routing alternatives for machine-to-machine networks, Journal of Network and Computer Applications 34 (5) (2011) 1587–1614.

[4] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, Journal of Network and Computer Applications 40 (2014) 325–344.

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

[6] J. Wang, Y. Liu, Y. Jiao, Building a trusted route in a mobile ad hoc network considering communication reliability and path length, Journal of Network and Computer Applications 34 (4) (2011) 1138–1149.

[7] 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.

[8] J.-L. Tsai, N.-W. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services, IEEE systems journal 9 (3) (2015) 805–815.

[9] Y. Liu, Y. Wang, 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 18 (10) (2017) 2740–2749.

[10] Q. Jiang, J. Ni, J. Ma, L. Yang, X. Shen, Integrated authentication and key agreement framework for vehicular cloud computing, IEEE Network 32 (3) (2018) 28–35.

[11] W. Shi, P. Gong, A new user authentication protocol for wireless sensor networks using elliptic curves cryptography, International Journal of Distributed Sensor Networks 9 (4) (2013) 730831.

[12] 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.

[13] M. A. Pandi Vijayakumar, A. Kannan, L. J. Deborah, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, IEEE Transactions on Intelligent Transportation Systems 17 (4) (2016).

[14] Y. Xiao, X. Shen, B. Sun, L. Cai, Security and privacy in rfid and applications in telemedicine, IEEE communications magazine 44 (4) (2006) 64–72.

[15] N. Kumar, K. Kaur, S. C. Misra, R. Iqbal, An intelligent rfid-enabled authentication scheme for healthcare applications in vehicular mobile cloud, Peer-to-Peer Networking and Applications 9 (5) (2016) 824–840.

[16] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, J. Shen, A lightweight and anonymous rfid tag authentication protocol with cloud assistance for e-healthcare applications, Journal of Ambient Intelligence and Humanized Computing 9 (4) (2018) 919–930.

[17] Y. Chen, J.-S. Chou, Ecc-based untraceable authentication for large-scale active-tag rfid systems, Electronic Commerce Research 15 (1) (2015) 97–120.

[18] K. Srivastava, A. K. Awasthi, S. D. Kaul, R. Mittal, A hash based mutual rfid tag authentication protocol in telecare medicine information system, Journal of medical systems 39 (1) (2015) 153.

[19] C.-T. Li, C.-Y. Weng, C.-C. Lee, A secure rfid tag authentication protocol with privacy preserving in telecare medicine information system, Journal of medical systems 39 (8) (2015) 77.

[20] N. Dinarvand, H. Barati, An efficient and secure rfid authentication protocol using elliptic curve cryptography, Wireless Networks 25 (1) (2019) 415–428.

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

[22] Y.-C. Chen, H.-M. Sun, 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, IEEE, 2014, pp. 25–27.

[23] D. He, N. Kumar, M. K. Khan, L. Wang, J. Shen, Efficient privacy-aware authentication scheme for mobile cloud computing services, IEEE Systems Journal 12 (2) (2016) 1621–1631.

[24] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet, IEEE Transactions on Vehicular Technology 65 (2) (2015) 896–911.

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

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

[27] R. Amin, G. Biswas, A secure three-factor user authentication and key agreement protocol for tmis with user anonymity, Journal of medical systems 39 (8) (2015) 78.