Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 1, pp. 217–237
DOI : 10.47974/JDMSC-2140

A suitable key agreement protocol for autonomous vehicle and digital twin using ECC

Fauzia Hassan *
School of Basic and Applied Sciences
Shobhit Institute of Engineering and Technology
Meerut 250110
Uttar Pradesh
India

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

Anil Kumar Nishad §
Department of Mathematics
School of Basic Sciences
Galgotias University
Greater Noida 203201
Uttar Pradesh
India

Mukesh Kumar Sharma ‡
Department of Mathematics
Chaudhary Charan Singh University
Meerut 250004
Uttar Pradesh
India

* *E-mail:* hassan.fauzia143@gmail.com
† *E-mail:* vkmaths@shyamlal.du.ac.in;(Corresponding Author)
vinod.iitkgp13@gmail.com
§ *E-mail:* anil.k.nishad16@gmail.com
‡ *E-mail:* drmukeshsharma@gmail.com

Pranav Dass [@]
Department of Computer Science
Shyam Lal College
University of Delhi
New Delhi 110032
India

Abstract

Autonomous vehicles (AVs) are transforming transportation, and their development and operation depend more and more on digital twins (DTs). DTs are virtual representations of AVs that can be used to replicate and test their behavior in various settings. Nowadays, protecting privacy and safety is a major concern because the integration of these technologies has resulted in both happy and catastrophic situations. We suggest an elliptic curve cryptography (ECC)-based key agreement method for AVs and DTs in this paper. We'll look at the key security improvements made so far, explore a number of attack methods, and assess the computational and communication costs inside the proposed framework. In addition, security analysis is used to ensure secure and efficient communication. Lastly, our findings indicate that the suggested protocol satisfies every security need compared to existing protocols.

Subject Classification (2010): *11T71, 94A60, 94A62.*

Keywords: *Autonomous vehicle, Security and privacy, Digital twin, Elliptic curve cryptography.*

1. Introduction

The concept of DT has arisen as a revolutionary force in the area of cutting-edge technology [1], altering the way we design, monitor and optimize complex systems. A digital depiction or replication of a tangible object, like a system, process, or product, is called a DT. In real time, this digital replica records the dynamic properties, interactions, and behavior of the physical thing. A DT is basically a bridge between the digital and physical realms, thus providing an excellent instrument for productivity and innovation across a range of business sectors.

DT is generated using data from sensors, cameras, and other devices that continuously monitor physical things or systems [2]. By simulating a physical object's or system's behavior in various scenarios, DTs can assist scientists and engineers in improving product design, streamlining the manufacturing process and forecasting maintenance requirements. Almost every industry uses DTs, including healthcare, manufacturing,

[@] *E-mail:* `pdasscs@shyamlal.du.ac.in`

architecture and so on. The critical relevance of guaranteeing secure communication and data integrity cannot be overemphasized in the fast-evolving field of AV and DT technologies.

1.1 *Components of DT*

Some of the components of DT are discussed in this section:

- **Physical entity:** The digital equivalent of the real-world system, process, or object. It may be a manufacturing machine, a car, a structure, or even an entire supply chain.
- **Virtual model:** The physical entity's digital representation. It may include data-based simulation, schematics, or 3D CAD models AI-based models, physics- or mathematics-based simulations, etc.
- **Sensors and IoT devices:** It collects real-time data from the physical object. Inputs are given, including operating status, vibration, temperature, and pressure are given. IoT sensors, cameras, GPS devices are a few examples.
- **Data integration and communication layer:** It sends data in real-time to the DT by the actual entity. Data from the physical world can now be moved to the virtual and vice versa. It utilizes cloud computing, edge computing, and IoT platforms.
- **Control systems:** This enables the physical object to receive commands or changes from the DT. Supporting feedback loops, optimization, and automation.

1.2 *Benefits of DT*

Some of the benefits of DT are discussed below:

- **Improved efficiency:** Automation of mundane tasks increases workflow and productivity.
- **Better customer experience:** Offers multichannel interaction, faster response, and personalized services.
- **Cost savings:** Reduces costs associated with running a business through streamlined processes and reduced waste of resources.
- **Competitive advantage:** Keeps companies innovative and relevant in the digital economy.
- **Scalability and flexibility:** It uses agile digital solutions to adjust to shifting market demands.

In the ever-changing transportation scene, the emergence of AVs is a game-changing technical advancement [3]. Autonomous or self-driving cars mark a paradigm change in the way we think about and engage with transportation networks. These advanced robots [4] differ from conventional cars in that they are equipped with high-level sensors, artificial intelligence, and strong control systems to move, perceive their environment, and make decisions without any human intervention. The search for safer, more efficient and more accessible transportation solutions drives the development of self-driving vehicles. The promise of a future [5] in which automobiles function autonomously is becoming more tangible as the automotive industry continues to invest extensively in research and development. The US National Highway Traffic Safety Administration classified automation into six stages [6]:

- The driver performs all duties at Level 0 and it is not automated.
- While maintaining an eye on the road, Level 1 assists the driver with various tasks like as braking and accelerator control.
- Level 2 is automated combination functions, where the vehicle is operated by two or more major control functions, relieving the driver of that responsibility. Examples of related functions are adaptive cruise control and lane centering.
- Level 3 includes a limited amount of automation for self-driving automobiles.
- High driving automation is provided by Level 4, where the driver only takes over when the automated situation becomes dangerous.
- Level 5 denotes complete automation, where the driver functions as a passenger and no human involvement is required.

As these systems become more interconnected, robust cryptographic techniques are necessary to protect personal data and ensure the ecosystem's overall dependability [7]. ECC is one such cryptographic method that has gained popularity due to its efficiency and security. ECC appears as an appropriate contender for tackling the security concerns posed by the dynamic and linked nature of AVs and their accompanying DTs due to its potential to deliver robust encryption with lower key lengths compared to previous cryptographic approaches [8].

This introduction investigates the need for a complex key agreement mechanism in various fields, highlighting potential vulnerabilities and risks associated with traditional techniques. Following that, it looks into

the benefits of ECC, emphasizing its applicability for resource-constrained contexts, which are frequently found in AV and DT systems. As we delve into the complexities of securing communication channels between AVs and their DTs [9], the proposed key agreement protocol seeks to address unique challenges such as latency, scalability and resource optimization. Figure 1 illustrates how AV and DT interact. The remainder of this exploration will delve into the major features of building an appropriate ECC-based key agreement protocol, explaining its implementation, benefits and ability to reinforce the security infrastructure of autonomous car and DT ecosystems. We hope to contribute to the growth of secure and dependable systems that pave the way for the smooth integration of these disruptive technologies into our daily lives by doing so.

1.3 *Literature review*

A survey article was proposed in 2019 by Kuutti et al. [10]. They provided a survey of deep learning-based methods for AV control in their study. Three categories were established for the approaches: simultaneous lateral and longitudinal control methods, longitudinal (acceleration and braking) and lateral (steering). Although there is some clear overlap between perception and vehicle control approaches, the focus of this work has been on the former. It was demonstrated that there has been a notable increase in research interest in this sector recently and this trend is anticipated to continue. A study on the requirements of DT-driven AV maintenance was proposed by Khan et al. [11] in the year 2020. Using the notion of the DT and recent advancements in machine learning, this paper examined autonomous maintenance. The information that resulted emphasized important requirements and how they can be satisfied. Generative learning is becoming popular in engineering applications and is a potentially significant enabling idea. A number of (digital) models have also been used by practitioners to track and diagnose issues at the system level. Unfortunately, the accuracy (and meaning) of models are impacted by the quality of the data utilized in this process and many potential users appear to lack the knowledge necessary to locate or utilize the appropriate data. A paper on the evolution of AVs was suggested by Alghodhaifi et al. [12] in 2021. This poll has reviewed all these above technologies to see how best they are used by vehicle-to-user (V2X) communication applications. The key features of this short-range communication technology are discussed, as well as how it can be used for some V2X applications including vehicle identification, forward collision

warning, and toll check that don't need high latency. They cannot, however, control applications such as remote driving and maintenance. Because of its low data rates and latency, it can deliver the most data overall and has the lowest delay of the four short-range technologies. Parekh et al. [3] published a review on AVs in 2022. They have discussed, highlighted, and analyzed technological advances of autonomous driving in this survey. They also looked into the most recent advancements in autonomous driving and case studies. Security, privacy, path planning, and safety

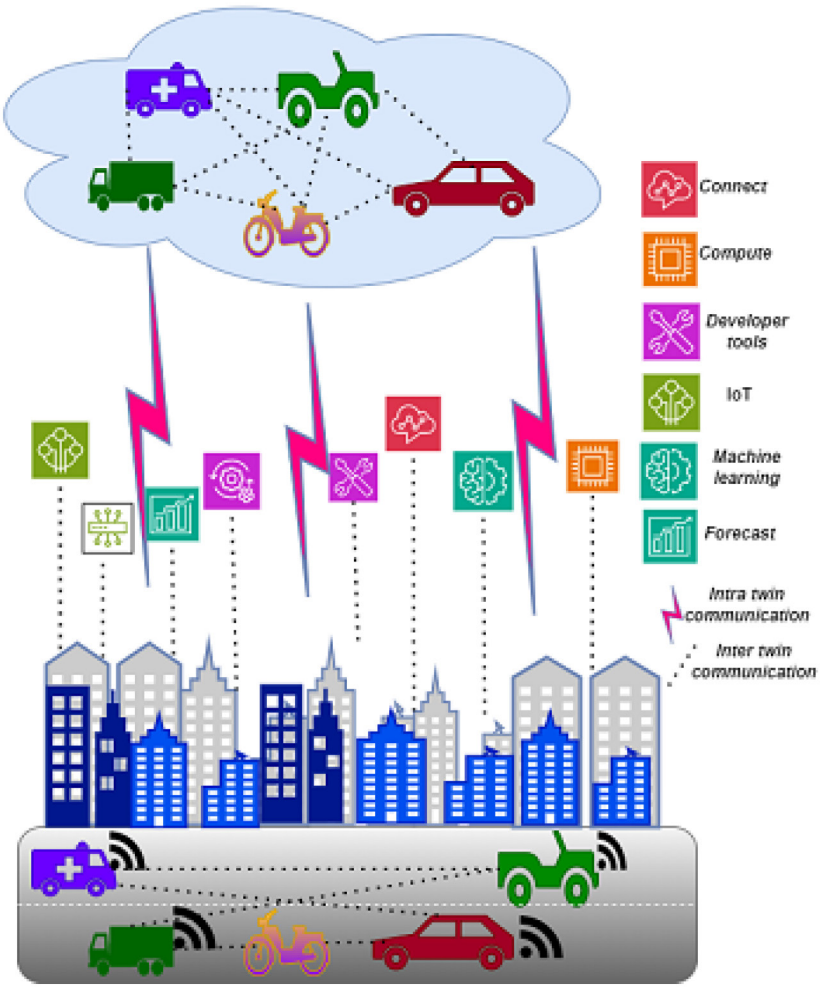

Figure 1

Interaction between AV and DT

problems associated with this study include quite a number of concerns. Consumer trust, governance, and human attitudes toward autonomous driving are examples of nontechnical issues that are important factors in the widespread adoption of AVs and related technology. A paper was recently proposed by Hossein et al. [13]. The development, history, and many stages of the application of DT technology are covered in this study. DT technologies that have been modified for usage in smart electric vehicle use cases are the main focus of this study. These technologies include autonomous motion control, cars as a service, driver aid systems, predictive mobility, vehicle-to-cloud-based driver assistance systems, and the Petri net model controversy.

1.4 *Security requirements for AV and DT interaction*

Strict security measures are necessary since the convergence of AV and DT produces a dangerous and complex environment. Ensuring the security of these systems is essential to preventing potential hazards, illegal access, and destructive behavior. By resolving these security needs, the integration of AVs and DTs can be done in a way that prioritizes the system's safety, privacy and reliability. To remain ahead of new threats and vulnerabilities, regular updates and communication with the larger cybersecurity community are required [14]. Security requirements for the AV and DT interactions are discussed below:

- **Confidentiality:** The protocol should provide a safe mechanism for the exchange of cryptographic keys between AVs and their DTs while keeping the keys confidential and resistant to eavesdropping.
- **Authentication:** To build mutual trust, both the AV and the DT must confirm each other's identities. This stops malicious actors from impersonating legitimate communication participants.
- **Non-repudiation:** Non-repudiation should be supported by the protocol, ensuring that no party involved in the communication can deny their involvement or the origin of a given message. This is critical for accountability in the event of a dispute or a security incident.
- **Resilience against replay attacks:** The protocol should include techniques to prevent replay attacks, in which an adversary intercepts and retransmits legal communications in order to fool the system. To do this, time-stamping or nonce usage can be used.

- **Scalability:** The protocol should be adaptable to handle the system's expanding number of AVs and DTs. It should run effectively as the network grows while maintaining security.

1.5 *Motivation and Contribution*

Modern transportation systems must be safe and dependable and this requires secure communication between autonomous cars and their digital duplicates. The security, efficiency, and scalability of conventional key agreement methods are frequently compromised, rendering them unfit for the rigorous demands of AV communication. ECC presents a viable solution because of its effective computing, small key sizes and robust security. A number of protocols pertaining to privacy and security concerns have been proposed. Before sharing sensitive data, entities must authenticate one another. Over the past few years, numerous ECC-based frameworks for key agreement and authentication have been proposed; however, they are all useless. In order to introduce a suitable key agreement for AVs and DTs utilizing ECC, we have presented a framework. The following attributes of the suggested framework are listed:

- We provide an ECC-based key agreement approach that works well for AVs and DTs.
- The session key is produced with the help of central authority.
- The paper explains the security analysis and security features.
- A comparison of the communication and computational costs of the proposed protocol with different schemes.

1.6 *Roadmap of the paper*

Section 1 includes the introduction, literature review, security requirements, motivation, and contribution of this study. Section 2 of this work analyzes the network and threat models, the mathematical concepts and notations used within the proposed protocol. Section 3 explains the explanation of the recommended protocol. Section 4 describes a security study of the proposed protocol, whereas Section 5 draws a conclusion of a performance analysis. Section 6 gives the conclusion and future discussion.

2. Mathematical terminologies

The terms and symbols used in the suggested protocol are defined in this section.

2.1 *Notations*

Table 1
Notations

Notations	Description	Notations	Description
EC	Elliptic curve	V_i	i^{th} Autonomous Vehicle
T_j	j^{th} Twin	ID_V	Identity of AV
PW_V	Password of AV	PW_T	Password of T_j
$h(.)$	Hash function	G	Elliptic curve group
M_V	Message sent by AV	M_T	Message sent by T_j
CA	Central authority	$\mathcal{A}$	Adversary
SK_{VT}	Session key of i^{th} AV	SK_{TV}	Session key of $j^{th}twin$
ΔT	Time delay in communication	$\cong$	Approximate value
$\Rightarrow$	Secure channel	$\rightarrow$	Public channel

This work makes use of the notations found in Table 1.

2.2 *ECC background over finite field*

Consider a prime finite field N_q of order q with a huge prime number q. An elliptic curve over N_q has the equation $s^2 = t^3 + ct + d \bmod q$, where c and d are elements of N_q [15, 14]. The additive elliptic curve group defined as $G = \{(t,s) : c, d \in N_q;\ (t,s) \in \mathcal{E}\} \cup \{\Phi\}$, where the point Φ is known as zero or identity element of G and G satisfies following operations [16]:

1. Let $R = (t,s) \in \mathrm{G}$ then define $-R = (t,-s)$ and $R + (-R) = \Phi$.
2. If $R = (t_1, s_1)$ and $S = (t_2, s_2) \in \mathrm{G}$, then $R + S = (t_3, s_3)$, where $t_3 = \mu^2 - t_1 - t_2 \bmod q$, $s_3 = \mu(s_1 - s_2) - s_1 \bmod q$ and

$$\mu = \begin{cases} \frac{s_2 - s_1}{t_2 - t_1} \mod q \text{ if } R \neq S \\ \frac{3t_1^2 + c}{2s_1} \mod q \text{ if } R = S \end{cases} \tag{1}$$

3. Let $R = (t, s) \in G$ then, scalar mortification of G is defined as: $n.R = R + R + R \ldots + R(n - times)$.
4. If g is the base point of G with order n, then $n.g = \Phi$.

2.3 *Network model*

We discuss the network model for the suggested work in this section. Three entities make up the model:

- **Autonomous vehicle (AV)**: AV is another name for a driverless vehicle. It does not require human aid to navigate or operate. These vehicles are equipped with contemporary technology and sensors that let them sense their environment, make independent decisions and control their movement. The primary purpose of AV is to deliver transportation that is safe, efficient and convenient.
- **Central authority (CA)**: The CA is an essential part in managing and controlling cloud infrastructure and services. It is in charge of creating policies, enforcing regulations, and making crucial choices that govern the behavior of the cloud environment.
- **Digital twin (DT)**: When viewed in a virtual environment, the digital representation closely resembles the equivalent physical counterpart in the real world.

2.4 *Threats model*

A threat model is a method of identifying, evaluating, and addressing potential security threats to a system, application, or process [17]. In this regard, it serves to help organizations understand what the risks are and, subsequently, develop strategies on how to mitigate or remove them.

It aims to capture the security characteristics of key exchange protocols, particularly when attackers are actively involved. According to the CK model, a key exchange protocol's security is defined so that the shared keys are safe even in the event that a hostile party deliberately tries to disrupt communication in an effort to jeopardise the confidentiality or integrity of the keys.

The model has been widely applied in the creation and assessment of numerous cryptographic protocols, offering a formal framework for assessing the security of key exchange protocols. It facilitates methodical and thorough reasoning about the security characteristics of these protocols by researchers and practitioners [18].

3. The proposed protocol

The proposed protocol contains the following phases:

3.1 *Initialization phase*

Table 2

Registration phase via secure channel

V_i	CA	T_j ($j^{th}Twin$)
Input $\{ID_V, PW_V\}$ Computes $h_1 = h(PW_V \| ID_V)$ Sends $M_V = \{ID_V, PW_V, h_1\}$ $\ldots\ldots\ldots\ldots\ldots\Rightarrow$		
	Verify $t_{A_1} - t_{V_1} \le \Delta T$ Sends $M_V = \{ID_V, PW_V, h_1\}$ $\ldots\ldots\ldots\Rightarrow$	
		Verify $t_{T_1} - t_{A_2} \le \Delta T$ Computes $h_2 = h_1(PW_V \| ID_V \| ID_T)$ Sends $M_T = \{h_2, ID_T\}$ $\Leftarrow\ldots\ldots\ldots\ldots\ldots$
	$t_{A_2} - t_{T_2} \le \Delta T$ Sends M_T $\Leftarrow\ldots\ldots\ldots\ldots\ldots$	
Verifies $t_{V_2} - t_{A_3} \le t$ Computes $h_3 = h_2 \oplus h_1$ Stores h_3 in database		

In the proposed protocol, *CA* selects a large prime number q and a prime finite field over the selected prime number, i.e. Z_q^*. *CA* also selects an equation $N_q(c,d) : s^2 = t^3 + cs + d \mod q$ over N_q where $4c^3 + 27d^2 \mod q \neq 0$, which holds the condition of non-singularity. *CA* chooses g as the base point of G along with a hash function $h(.)$, which is defined as $h_i = \{0,1\}^* \rightarrow \{0,1\}^l$. Then *CA* publishes the parameters $\{N_q, EC, g, h(.), q\}$

3.2 *Registration phase*

In this phase, registration is done in the following manner:

Step 1: To register with *CA*, V_i inputs its ID_V and PW_V and computes $h_1 = h(PW_V \parallel ID_V)$ and sends M_V to CA via secure channel where M_V contains $\{ID_V, PW_V, h_1\}$.

Step 2: On receiving M_V, CA first verifies $t_{A_1} - t_{V_1} \leq \Delta T$ and if verifies, CA transfers M_V to T_j.

Step 3: T_j receives M_V and verifies whether $t_{T_1} - t_{A_2} \leq \Delta T$. If yes, then T_j computes $h_2 = h_1(PW_V \parallel ID_V \parallel ID_T)$ and sends M_T to CA via secure channel where M_T contains $\{h_2, ID_T\}$

Step 4: After receiving M_T, CA verifies $t_{A_2} - t_{T_{A_2}} \leq \Delta T$ and if verified CA transfers M_T to V_i.

Step 5: After receiving M_T from CA, V_i first verify whether $t_{V_2} - t_{A_3} \leq \Delta T$ and computes $h_3 = h_2 \oplus h_1$. Finally, V_i stores h_3 in database.

The registration process is described in Table 2:

3.3 *Login and authentication phase*

In order to enable more connections, V_i and T_j authenticate one another via CA at this phase and create a session key between them. The steps that are involved in the procedures are described below:

Table 3

Login and authentication phase via public channel

V_i	T_j ($j^{th}Twin$)
Inputs $\{ID_V^*, PW_V^*\}$	
Computes $h_1^* = h(PW_V^* \| ID_V^*)$	
Computes $h_3^* = h_2 \oplus h_1^*$	
Verifies $h_3^* = h_3$; If yes	
Computes $W_1 = h((ID_T \oplus PW_V) \| ID_V)$	
Generates $a \in Z_q^*$	
Computes $A = ag$	
Sends $M_1 = \{A, W_1, T_1\}$	
$\cdots\cdots\rightarrow$	
	Verifies $T_2 - T_1 \le \Delta T$
	Computes $W_1^* = h((PW_A \oplus ID_T) \| ID_V)$
	Verifies $W_1^* \stackrel{?}{=} W_1$, If yes
	Generates random value $b \in Z_q^*$
	Computes $B = bg$
	Computes $SK_{TV} = h(ID_T \| ID_V \| b.A \| T_3)$
	Computes $W_2 = h(A \| B \| (ID_V \oplus ID_T))$
	Sends $M_2 = \{W_2, B, T_3\}$
	$\leftarrow\cdots\cdots$
Verifies $T_4 - T_3 \le \Delta T$, If yes	
Computes $W_2^* = h(A \| B \| (ID_V \oplus ID_T))$	
Verifies $W_2^* \stackrel{?}{=} W_2$, If yes	
Computes $SK_{VT} = h(ID_V \| ID_T \| a.B \| T_3)$	

Step 1: V_i inputs ID_V^*, PW_V^* and computes $h_1^* = h(PW_V^* \| ID_V^*)$, further V_i computes $h_3^* = h_2 \oplus h_1^*$ and verifies whether $h_3^* \stackrel{?}{=} h_3$. If the condition is satisfied, then V_i computes $W_1 = h((ID_V \oplus PW_T) \| ID_V)$ and generates a random value $a \in Z_q^*$ and computes $A = a.g$ and finally V_i sends $M_1 = \{A, W_1, T_1\}$ to T_j via public channel.

Step 2: Upon receiving M_1, T_j verifies $T_2 - T_1 \leq \Delta T$ and computes $W_1^* = h((PW_A \oplus ID_T) \| |D_V)$ and verifies $W_1^* \stackrel{?}{=} W_1$, if yes then T_j generates a random value $b \in Z_q^*$ and computes $B = b.g$ then T_j computes the session key $SK_{TV} = h(ID_T \| ID_V \| b.A \| T_3)$. Further, T_j computes $W_2 = h(A \| B \| (ID_V \oplus ID_T \| T_3))$. Then T_i sends $M_2 = \{W_2, B, T_3\}$ to V_i via public channel.

Step 3: Upon receiving M_2, V_i verifies $T_4 - T_3 \leq \Delta T$ if yes, then computes $W_2^* = h(A \| B \| (ID_A \oplus ID_T))$ and verifies whether $W_2^* \stackrel{?}{=} W_2$. If yes, then V_i calculates its session key $SK_{VT} = h(ID_V \| ID_T \| a.B \| T_3)$.

Hence, after validating one another, V_i and T_j decided on a common session key, $SK_{VT} = SK_{TV} = SK$. This process is shown in Table 3.

4. Security analysis

Security analysis is a broad and systematic assessment of vulnerabilities, risks, and any existing measures to ensure what can be done against prospective threats in a system or application or organization. Below are some informal security analysis are discussed:

4.1 *Replay attack*

A replay attack attempts to fool a system by convincing it that the replayed data is real and still relevant. This form of attack assumes that the communication between two parties is safe and has not been interfered with. We should employ unique time stamps and unique random numbers at every stage. The proposed protocol checks each step to whether the message is sent on time or not. Time stamps and secure hash functions included in our framework form its basis of security into every stage of the login and authentication procedure. This incorporation presents $\mathcal{A}$ with a significant barrier, making a repeat effort quite difficult. Individual $\mathcal{A}$ will not be able to access or recognize the secure data if they try to replay the intercepted communication delivered over an unsecured channel. Thus, the method we have outlined is secure against replay attacks.

4.2 *Anonymity property*

Individuals can engage in activities or transactions without exposing their genuine identity, providing privacy and protection from unwanted observation. This attribute is important in a variety of situations, including online interactions, financial transactions, and communication systems. In the proposed protocol, except for the time stamps T_1 and T_3, the exchanged messages in the proposed protocol are $M_1 = \{A, W_1, T_1\}$ and $M_2 = \{B, W_2, T_3\}$. The rest of the information in these messages is encrypted or the result of a one-way hash function and randomized by fresh nonce values. Consequently, this protocol proposed ensures anonymity in the sense that the messages exchange does not disclose any information.

4.3 *Man in middle attack*

For the man in middle attack, the $\mathcal{A}$ secretly interrupts and possibly alters the communication between the two parties who believed they were directly communicating with each other. The proposed protocol in each step includes time stamps and various hash functions, which is quite well-known that it is hard to come up with a hash function under the collision-free condition of one-way hash functions. Therefore, the suggested protocol is man-in-the-middle attack protected.

4.4 *Forward secrecy attack*

Forward secrecy, or Perfect Forward Secrecy (PFS), is an attribute of a cryptographic system that ensures that the confidentiality of past communications is not compromised by the compromise of long-term secret keys. Forward secrecy ensures that previously transmitted messages remain private even if the current or future cryptographic keys are compromised. The proposed protocol only uses ECC, along with a secure collision-resistant hash function.

4.5 *Insider attack*

Insider attacks underscore the importance of a complete and proactive cybersecurity strategy, recognizing that threats can come from both external and inside sources. An insider attack, according to the proposed protocol, is a security breach done by someone who has genuine authorised access to an organization's network, systems or data. The authentication method in the proposed protocol is carried out by participants using their

own secret keys. As a result, the proposed approach is resistant to stolen verifiers and insider threats.

4.6 *Key freshness*

The fundamental purpose of key freshness is to improve the security of encrypted communication by reducing the time a single key is in use. This practice helps to limit the dangers associated with exposing cryptographic keys to prospective assaults over time. The new nonce was created at every step, and verification time stamps were performed in the protocol. The time stamps with a random nonce are different in every session stamp. So the uniqueness of the key authenticates the freshness of the key protocol.

4.7 *Untraceability*

In the context of digital transactions and communication, untraceability is frequently related to privacy and anonymity. It is the attribute that makes tracing a specific activity or transaction back to the originator or participant difficult or impossible. In certain applications where consumers value privacy, confidentiality, and anonymity, untraceability is a desired attribute.Two features are included in the proposed protocol. The hacker is unable to distinguish between users initial identities, nor can he identify whether two independent sessions that begin at different times belong to the same individuals.

4.8 *Session key agreement*

The proposed protocol contains session keys where V_i calculates its session key $SK_{VT} = h(ID_V \| ID_T \| a.B \| T_3)$ and T_j computes its session keys $SK_{TV} = h(ID_V \| ID_T \| b.A \| T_3)$ and finally $SK_{VT} = SK_{TV}$ which ensures that the proposed protocol contains crytographic property.

4.9 *Mutual authentication*

In the proposed scheme, AV computes $H_1 = h(ID_A \| ID_T \| PW_A)$ and sends it to T_j. Now, T_j verifies whether $H_1^* \stackrel{?}{=} H_1$ and computes $H_2 = h(X \| Y \| ID_A \oplus ID_T \| T_3)$ and then sends it to AV. AV verifies whether $H_2^* = H_2$ and finally computes the session key. Thus, AV and T_j mutually authenticate each other and the proposed framework achieves this mutual authentication.

5. Performance analysis

The security characteristics, communication costs, and computational costs of the suggested protocol like [23] are compared in the section that follows in order to determine how well it performs. Additionally, some schemes have computational costs that are less than those of the suggested protocol, but they are unable to offer alternative security attacks.

5.1 *Security features*

A security analysis is required to compare the behavior of the proposed protocol in comparison with schemes that have been presented earlier in the same category. To check whether it is secure or not, comparisons of security features are in order and are to show that they can withstand attack and survive attacks. Table 4 shows the security features of the proposed protocol and the existing protocols like [19, 20, 21, 22]. In that table, the proposed protocol is more secure and suitable for the twin-system environment. Security features comparison

Table 4

Security features comparison

Security features	[19]	[20]	[21]	[22]	Proposed
RA	√	√	√	√	√
AP	×	√	√	×	√
PSA	√	√	×	√	√
DA	√	×	√	×	√
MA	×	√	×	√	√
SKA	√	×	√	√	√
KF	√	×	√	×	√
UN	√	√	√	√	√
FSA	×	√	×	√	√
SFV	√	√	×	√	√
IA	√	×	√	√	√
PB	√	√	√	×	√

Note ×**:** Fails to stop the attack and √ Stops the attack, *RA*: Replay attack, *AP*: Anonymity Property, *PSA*: Parallel session attack, *DA*: Data Authentication, *MA*: Message authentication, *PK*: Provision of key agreement, *KF*: Key freshness, *UN*: Untraceability, *RP*: No secure channel in registration phase, *FK*: Fails to protect session key, *IA*: Insider attack, *PB*: Password based protocol

5.2 *Communication cost*

It's the number of bits being exchanged between them during execution that determines the communication cost. In the proposed protocol, we use communication costs from Wu et al.'s scheme in [23]. The details of some of the operations are:

- Random number: 160 bits
- for Encryption/decryption and ECC point: 320 bits
- Identifier: 64 bits
- Output of hash function: 256 bits
- Time stamp: 32 bits

Comparison among the communication cost and computational comparison with different protocols like [19, 20, 21, 22] are provided in Table 5. It shows that, compared to other schemes provided, the suggested framework has a reduced communication cost. Therefore, we draw the conclusion that the suggested scheme offers the best security features and has a significantly lower communication cost than the others.

Table 5

Communication cost and Computational cost of different schemes

Scheme	Communication costs (bits)	Computational costs (in ms)
Son et al. [19]	4672	$10T_{hp} + 2T_{bp} + 8T_{mul} \cong 563.8$
Khatoon et al. [20]	5664	$2T_{bp} + 11\,T_{mul} + 2T_{add} \cong 347.1$
Sengupta et al. [21]	2624	$4T_{hp} + 2T_{bp} + T_{mul} \cong 227.7$
Thakur et al. [22]	4672	$10T_{hp} + 7T_{mul} + 2T_{bp} \cong 476.3$
Proposed	1472	$6T_{hp} + 2T_{mul} \cong 279.6$

5.3 *Computational cost*

In particular, we make reference to the tests conducted in [23], which make use of a Java pairing-based cryptography library. An Intel Core i5-8300H quad-core processor with 16GB of RAM was used for the experiment. Below is a summary of the symbol significance that was utilised in the performance comparisons:

- T_{hp}: String-to-point hash operation computational cost ≅ 42.1 ms.
- T_{exp}: Modular exponential operation computational cost ≅ 15.8 ms.
- T_{mul}: Point scalar multiplication operation computational cost ≅ 13.5 ms.
- T_{bp}: Bilinear pairing operation computational cost ≅ 17.4 ms.
- T_{fe}: Fuzzy extractor computational cost ≅ 13.5~ms.

Since an exclusive-OR operation has a comparatively low computational cost, we have disregarded it in this case. Table 5 shows the computational cost of the proposed protocol and some previous schemes like [19, 20, 21, 22]. Here, the computational cost for the proposed protocol is 279.6~ms, which is less than Son et al.'s [19], Khatoon et al.'s [20], Thakur et al.'s [22] but greater than Sengupta et al.'s [21]. The computational cost for the proposed protocol is more less than the existing protocol, which is shown in Table 5.

6. Conclusion and future scope

ECC to design and implement an appropriate key agreement mechanism for DTs and AVs represents a critical step in guaranteeing the security and integrity of communications in dynamic, networked systems. The suggested protocol aims to provide a strong basis for secure key exchange between AVs and their DTs by attending to the particular security concerns previously mentioned. The paper shed some light on the growing use of AV and DT and the various security and privacy issues regarding the safety of these two emerging technologies. The proposed protocol provides a key agreement among AVs and DTs using ECC. Additionally, when compared to other proposed schemes, the suggested protocol is secure against a variety of security vulnerabilities, including replay attacks, man-in-the-middle attacks, data authentication, anonymity, untraceability, insider attacks, and more. It is readily apparent that the proposed protocol has low communication and computation costs when compared to competing systems. We expect the proposed method to be helpful to AV and DT researchers in future.

References

[1] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects," *IEEE Internet Things J.* (2023).

[2] G. Bhatti, H. Mohan, and R. R. Singh, "Towards the future of smart electric vehicles: Digital twin technology," *Renew. Sustain. Energy Rev.*, vol. 141, p. 110801 (2021).

[3] D. Parekh, N. Poddar, A. Rajpurkar, M. Chahal, N. Kumar, G. P. Joshi, and W. Cho, "A review on autonomous vehicles: Progress, methods and challenges," *Electronics,* vol. 11, no. 14, p. 2162 (2022).

[4] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A survey of autonomous vehicles: Enabling communication technologies and challenges," *Sensors,* vol. 21, no. 3, p. 706 (2021).

[5] R. Roriz, J. Cabral, and T. Gomes, "Automotive lidar technology: A survey," *IEEE Trans. Intell. Transp. Syst.,* vol. 23, no. 7, pp. 6282–6297 (2021).

[6] M. Vagia, A. A. Transeth, and S. A. Fjerdingen, "A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed?," *Appl. Ergon.*, vol. 53, pp. 190–202 (2016).

[7] C. He, T. H. Luan, R. Lu, Z. Su, and M. Dong, "Security and privacy in vehicular digital twin networks: Challenges and solutions," *IEEE Wireless Commun.* (2022).

[8] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *J. Interdiscip. Math.,* vol. 23, no. 2, pp. 463–470 (2020).

[9] X. Luo, J. Wen, J. Kang, J. Nie, Z. Xiong, Y. Zhang, Z. Yang, and S. Xie, "Privacy attacks and defenses for digital twin migrations in vehicular systems," [article in progress].

[10] S. Kuutti, R. Bowden, Y. Jin, P. Barber, S. Fallah, "A survey of deep learning applications to autonomous vehicle control," *IEEE Trans. Intell. Transp. Syst.,* vol. 22, no. 2, pp. 712–733 (2020).

[11] S. Khan, M. Farnsworth, R. McWilliam, and J. Erkoyuncu, "On the requirements of digital twin-driven autonomous maintenance," *Annu. Rev. Control,* vol. 50, pp. 13–28 (2020).

[12] H. Alghodhaifi, and S. Lakshmanan, "Autonomous vehicle evaluation: A comprehensive survey on modeling and simulation approaches," *IEEE Access,* vol. 9, pp. 151531–151566 (2021).

[13] S. M. Hossain, S. K. Saha, S. Banik, and T. Banik, "A new era of mobility: Exploring digital twin applications in autonomous vehicular systems," in 2023 IEEE World AI IoT Congress (AIIoT), IEEE, pp. 0493–0499 (2023).

[14] V. Kumar, "RSFVC: Robust biometric-based secure framework for vehicular cloud networking," *IEEE Trans. Intell. Transp. Syst.* (2023) (in press).

[15] O. Benamara, "Algorithms for elliptic curves," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 2, pp. 455–462 (2022).

[16] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "LAKAF: Lightweight authentication and key agreement framework for smart grid network," *J. Syst. Archit.,* vol. 116, p. 102053 (2021).

[17] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in Proc. Int. Conf. Theory Appl. Cryptogr. Tech., Springer, pp. 453–474 (2001).

[18] A. A. Khan, V. Kumar, J. Srinivas, S. Kumari, M. K. Gupta, "RAKS: Robust authentication and key agreement scheme for satellite infrastructure," *Telecommun. Syst.,* vol. 81, no. 1, pp. 83–98 (2022).

[19] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, "On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain," *IEEE Access,* vol. 10, pp. 75365–75375 (2022).

[20] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE Access,* vol. 7, pp. 47962–47971 (2019).

[21] A. Sengupta, A. Singh, P. Kumar, and T. Dhar, "A secure and improved two-factor authentication scheme using elliptic curve and bilinear pairing for cyber-physical systems," *Multimed. Tools Appl.,* vol. 81, no. 16, pp. 22425–22448 (2022).

[22] G. Thakur, P. Kumar, S. Jangirala, A. K. Das, and Y. Park, "An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment," *IEEE Access,* vol. 11, pp. 26877–26892 (2023).

[23] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, "An enhanced pairing-based authentication scheme for smart grid communications," *J. Ambient Intell. Humanized Comput.,* pp. 1–13 (2021).

Received November, 2023