Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

A Digital Twin-Based Safe Authentication Protocol for Vehicular Cloud Networking

Dheeraj Tiger[1,3], Vinod Kumar[2,*], Anshu Malhotra[3]
[1]*Department of Mathematics, Rajdhani College, University of Delhi-110055, India*
[2]*Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi-110032, India*
[3]*Department of Mathematics, School of Applied Science, North cap University, Gurugram-122017, India*
**: Corresponding author (E-mail: vkmaths@shyamlal.du.ac.in & vinod.iitkgp13@gmal.com)*

Abstract:- Diverse services have been made possible by the swift expansion of autonomous vehicles; nonetheless, real-time sensing, pro- cessing, and communication overheads sometimes result in an unsatisfactory passenger experience. Our proposal utilizes cloud computing technologies to facilitate information integration and computation for autonomous vehicles, as we want to tackle these issues using a revolutionary vehicular digital twin framework. To create feedback, our method updates digital data on the cloud and synchronizes it in real time with autonomous cars. Ensuring comprehensive communication security and privacy protection is necessary to enable the real-time information synchronization of autonomous automobiles and digital twins in an open communication environment. Our proposal is to create a safe structure for data interchange between autonomous vehicles and digital twins in order to allay these worries. We discuss the security analysis of the proposed scheme. Compared to current vehicular communication protocols, we show that our proposed protocol has lower computing and communication overheads and may be applied to scenarios including digital twins. Through the reduction of communication overheads, our proposed approach improves the overall passenger experience while also addressing security and privacy concerns related to data exchange between digital twins and autonomous vehicles. The advancement of autonomous vehicles and how they are incorporated into our daily lives will be greatly impacted by our study.

Keywords*: Digital Twin, Elliptic curve cryptography, Autonomous vehicle, Security, Privacy*

1. Introduction

With a lot of help from industry and academics, autonomous driving research has moved quickly in the last several years. Firms like Tesla, Volvo, and Toyota have made significant investments in the development and investigation of self-driving cars, and most newly launched car models already have Level 2 autonomy. The autonomous vehicle (AV) is outfitted with a range of sensors and computer units that function as a mobile computing platform. These components are designed to detect and process environmental elements such as road laws, obstacles, pedestrians, and meteorological data. By modifying its speed and route to avoid traffic and provide a comfortable ride for its passengers, the AV can now make decisions about driving in real time. However, an autonomous vehicle's resources may be severely taxed by real-time sensing, processing, and communication, which could lead to errors and accidents or even a bad passenger experience. Furthermore, an AV cannot predict traffic conditions outside of its field of vision because of its restricted communication range. We suggest a vehicular digital twin authentication key agreement architecture as a solution to these problems, which offers vital assistance for AV information fusion and computing.

Specifically, we suggest an online virtual vehicle model named *iTwin* that functions as a digital twin (DT) of the real-world model shown in Fig. 1. Essential information like preferred routes and destinations, information about neighbouring roads, and driving habits are all gathered

y the *iTwin* from its *AV*. Then, in order to save the processing capabilities of the physical *AV*, real-time computations are carried out on the cloud and feedback is sent to it. Together with exchanging road data and sending it to their physical counterparts, the cloud-based iTwins can also interact with other digital twins in all other AVs. iTwin communications can greatly enhance the physical communication systems of AVs at a low cost, with configurable ranges ranging from line-of-sight to city-wide. Our suggested framework can improve the entire

driving experience for passengers and simultaneously improve the safety and performance of autonomous vehicles by utilizing digital twin technology. We think our framework can play a major role in the field of autonomous driving and help this fascinating technology continue to grow and progress.

1.1. Motivation and contribution

The safety of autonomous vehicles may be seriously jeopardized if security concerns like privacy protection and trustworthy communication are not addressed in a comprehensive manner. This is due to the fact that private information is shared and open lines of communication exist between iTwin and its physical master. For example, the position or identity of an honest AV can be used to track it; both AV and iTwin are unable to ascertain the veracity of the messages they receive. To overcome the aforementioned problems, we propose anonymous authentication. Unforgeability and conditional traceability, on the other hand, are two further problems that require attention. In particular, an iTwin will reveal its true identity if it transmits a fraudulent message because it can only recognize and accept information from its physical master. To effectively address the previously identified issues, we offer a secure authentication technique built on elliptic curve cryptography. The following is a summary of our primary contributions in this paper:

- Our proposal is a strong mutual authentication system that reduces the communication and computation expenses for all parties involved in digital twin vehicular communication. Lightweight procedures like hash functions and ECC scaler multiplications are heavily utilized in the suggested system.
- We formally demonstrate the security of the suggested schemes under the ROR paradigm and contrast them with pertinent traditional authentication solutions. Our technique is especially suitable for digital twin vehicular communication applications since it satisfies all security evaluation criteria with the least amount of computation and communication overhead.
- To show that the suggested protocol is more secure and efficient than existing methods in digital twin vehicular communication, it is compared to several competing contemporary protocols [1, 2, 3, 4].
- The proposed system can withstand various security attacks, as shown by the informal security assessment, which enables its application in a real-world digital twin vehicular communication.

1.2. Related works

The development of the Internet of Vehicles (IoV) has been made possible by the digital twin (DT) technologies with Internet of Things (IoT), which allow for the efficient and convenient real-time data sharing among different stakeholders in the vehicular network. In order to assess the efficacy of various IoV navigation strategies employing DTs with a mobility model, Zhang et al. [5] dynamically simulated charging stations with mobile Electric Vehicles (EVs). In order to enhance transportation management in the Internet of Vehicles, Bhatti et al. [6] created a complex EV DTs system. Information integrity and confidentiality are compromised by intermediates, which raises security concerns with IoV data transfer protocols between IoV nodes. For Internet of Vehicles (IoV) data communication, symmetric encryption methods like “Data Encryption Standard and Advanced Encryption Standard” are commonly employed. They can be used in encryption scenarios where there are high data volumes and stringent real-time requirements because of their speedy speed and low computation necessary. Asymmetric encryption methods, such elliptic curve and ElGamal cryptography, offer higher security because they only require the public key to ensure data transmission security and only store the private key on the node. The Ad Hoc Vehicular Network’s information transmission rate was greatly enhanced by Sellami and Alaya’s [7] efficient key management system, which was based on symmetric and asymmetric encryption. La Manna et al.[8] increased the security of wireless update features in the automobile sector by implementing an attribute-based encryption approach in automotive software and hardware platforms. Xu et al. [9] proposed a bi-linear mapping approach-based authentication key agreement framework for vehicular digital twin communication. On the other hand, comprehensive research on DTs modeling requirements under the IoV and Cyber-Physical System is lacking. This study suggests particular DTs modelling techniques and an asymmetric encryption security plan for data transfer to address these problems, ensuring data security and cutting down on the time required for data encryption and decryption. These developments have the potential to greatly enhance the security of IoV vehicular digital twin communication.

2.System Model

Autonomous vehicles (AVs), a central authority (CA), and related cloud-based iTwins make up the system model for our suggested architecture for vehicle digital twin communication, as illustrated in Fig. 1. Each participant's salient characteristics and security needs are listed in the following information:

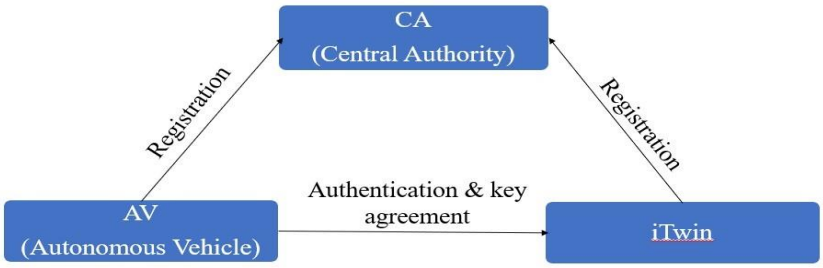
- **Central Authority (CA):** The CA is in charge of generating secret keys and pseudonyms for each AV and $iTwin$ in the system. In addition, it is in charge of granting each iTwin a group certificate that enables communication with other $iTwins$ following a successful AV authentication. In the event of erroneous messages or security breaches, the CA must be able to locate and trace the authentic identities created by iTwins.
- **Autonomous Vehicle (AV):** To raise the caliber of service, the AV talks with each $iTwin$ and gathers data from its installed sensors. Before connecting to any iTwin, it must verify itself with the CA and make sure that secure communication channels are in place to safeguard the confidentiality and integrity of the data it transfers.
- **iTwin:** To improve passenger happiness overall, the $iTwin$ provides computational services based on data col- lected from its linked physical vehicle. In order to safeguard the confidentiality and integrity of the data it receives and sends; it must first verify itself with the CA before establishing a secure communication channel with the AV.

We need safe authentication and communication amongst all participants in order to guarantee the security of the proposed framework. For each AV and $iTwin$, the CA must create strong pseudonyms and secret keys in order to thwart impersonation attempts. Depending on the urgency and sensitivity of the data, all communication routes between the $AV, iTwins,$ and CA need to be encrypted using either symmetric or asymmetric encryption methods. Furthermore, in order to avoid any security lapses or miscommunications, the CA needs to be able to monitor authentic identities created by $iTwins$. The confidentiality and integrity of data flow in our framework for vehicle digital twin communication may be guaranteed by putting these security measures into place.

2.1. Attacker Model

It is essential to carefully evaluate any potential security vulnerabilities given the high-risk nature of the DT network. To examine the mutual authentication and session key negotiation process, we use the "Dolev-Yao (DY) threat model" [10] in this study. The adversary model put forward by Canetti and Krawczyk (CKM) [11] is also included. The CKM paradigm increases the attacker's power by enabling them to obtain temporary credentials that are session-specific, which may result in the revelation of the session key that was agreed upon by the involved parties. A more thorough examination of the adversary's possible capabilities inside the system is provided by this model. We may evaluate the security of the mutual authentication and session key negotiation process in the DT network while taking into account a variety of possible threats and adversaries by utilizing the DY threat model and adding the CKM adversary model.

Figure 1: System model [16]



2.2. Paper organization

This is the format for the remaining portion of the paper. We address the crucial preliminary work associated with the suggested vehicle digital iTwin communication framework in Section 3. Our suggested authentication and secure communication mechanism for iTwins and autonomous cars is presented in Section 4. Our protocol is

thoroughly analysed for security in Section 5, which also includes the outcomes of a Scyther tool simulation. The analysis of our suggested framework's throughput, latency, and energy usage is presented in Section 6. The paper is finally concluded in Section 6, where we address future directions for this field of research as well as summarize the contributions of our work.

3. Mathematical preliminaries

In order to properly examine and explain the proposed framework, we lay out the necessary mathematical techniques and notation in this section.

3.1 Notation table

The important notation that are utilized in the proposed framework are shown in Table 1.

3.2 Background of Elliptic Curve Cryptography (ECC)

ECC is a cryptographic method that uses public key encryption based on an elliptic curve over a large finite field. Even with lower key lengths than classical public-key cryptography, ECC provides better security and performance [12, 13]. Let q be a prime number of significant magnitudes, and a, b ∈ Z∗ $a, b \in Z\_q\hat{}*$, where $Z\_q\hat{}*$ represents a finite field. Assuming $4a\hat{}3 + 27b\hat{}2 \neq 0 \pmod{q}$, we can define a non-singular elliptic curve $E\_q\,(a,b)$ over the finite field $Z\_q\hat{}*$, q using the equation:

Table 1: Symbol and their meaning

Symbol	Meaning	Symbol	Meaning
EC	Elliptic curve	SK	Session Key
A	Attacker	$E_q(a,b)$	Elliptic curve over finite prime field F_q
G	EC based additive group	CA	Central authority
Q	Prime number	AV	Autonomous vehicles
$iTwin$	$iTwin$ vehicular cloud	$h(.)$	Hash function
$\|$	Concatenation operation	$\triangle T_i$	Time span
$\oplus$	Xor operation	g	The base point of the G
ID_A	Identity of A	PW_A	Password of A

$$E\_q(a,b) : y\hat{}2 \equiv x\hat{}3 + ax + b\ (mod q)$$

The additive group G associated with the elliptic curve is defined as $G = \{(x,y): x,y \in Z\_q\hat{}*, (x,y) \in Eq\} \cup \{\Theta\}$. As the identical element (zero element) inside G, Θ denotes the asymptotic point in this case. The operations on the group G′ are as follows [14]:

- **Scalar Multiplication:** Let X be a base point on the elliptic curve $Eq(a,b)$. The scalar multiplication operation is defined as:

  $$k \cdot X = X + \ldots + X \ (k\ times)$$, where k ∈$Z\_q\hat{}*$ is a positive integer.

- **Point Addition:** For $U = (x_1, y_1)$, $V = (x_2, y_2) \in G$, the addition of U and V is denoted as $U + V = (x_3, y_3)$, where: $x_3 = \ell^2 - x_1 - x_2 \ (mod\ q)$ and $y_3 = (\ell(x_1 - x_3) - y_1) \ (mod\ q)$ and ℓ is defined as:

  $$\ell = \begin{cases} (y_2 - y_1)/(x_2 - x_1) \quad mod\ q\ if\ U \neq V \\ (3x\hat{}2 + a)/(2y_1) \quad if\ mod\ q\ U = V \end{cases}$$

- **Point Negation:** For $X = (x,y) \in G$, the negation of is defined as $-X = (x, -y)$.

4. The proposed protocol

The proposed protocol contains following phases:

4.1 Initialization phase

CA plays the rule of public/private key generator or play the rule of third party. The following steps are doing in the initialization phase:

- CA chooses the non-singular EC as $Eq(a,b): y^2 = x^3 + ax + b\,(mod\ q)$.
- Selects g as the group generator of G. Chooses random value $c \in Z_q^*$ which is secret key for CA and set public key $PK_C = cg$.
- Chooses secure hash function.
- AV chooses $a \in Z_q^*$ and set it as his/her private key and calculates $PK_A = ag$ as public key.
- $iTwin$ chooses random number $k \in Z_q^*$, set as a private key and set public key $PK_{iT} = kg$.

4.2. Registration phase

In order to obtain the information needed for communication with the DT-vehicular network, AV and $iTwin$ must register through the CA. A crucial agreement between AV and iTwin and CA is required. This is a detailed description of the AV and $iTwin$ registration phase:

Step 1. AV input his identity ID_A and password PW_A and computes $H_{R1} = h(PW_A \| ID_A)$, sends $\{ID_A, PW_A, H_{R1}\}$ to CA via secure channel.

Step 2. On receiving the above information, *CA* generates $C_T \in Z_q^*$. Then CA sends $\{ID_A, PW_A, H_{R1}, C_T\}$ to $iTwin$ through secure.

Step 3. On receiving the above message, $iTwin$ inputs own identity ID_T, $iTwin$ computes $H_{R2} = H_{R1} \oplus h(ID_T \| ID_A)$ and sends $\{H_{R2}, ID_T\}$ to CA via secure channel.

Step 4. On receiving the above message from $iTwin$, CA generates $C_A \in Z_q^*$. Then sends $\{H_{R2}, ID_T\}$ to AV.

Step 5. On receiving $\{H_{R2}, C_A\}$, *AV* computes $H_{R3} = H_{R2} \oplus h(ID_T \| ID_A)$. Finally, *AV* stores H_{R3} in database.

4.3. Login and authentication phase

Following registration, AV and $iTwin$ generated a shared session key by authenticating against one another. The following are the specifics of the login and authentication phase:

Step 1. *AV* login with identity ID_A^* and password PW_A^* and computes $H_{R1}^* = h(PW_A^* \| ID_A^*)$. *AV* verifies $H_{R3} ?= H_{R1}^*$ if yes then AV generates a $\in Z_q^*$. AV computes $W_1 = h(ID_A \| C_A \| ID_T)$ and $K_1 = h(PW_A \| ID_T)$. Then, AV encrypts (ag, W_1, C_A) with K_1as $E_1 = E_{K_1}(ag, W_1, C_A)$. Finally, AV sends $M_1 = \{E_1, T_1\}$ to $iTwin$.

Step 2. On receiving $M_1 = \{E_1, T_1\}$ from *AV*, first $iTwin$ verifies timestamp $t_2 - t_1 \leq \triangle t$ aborts if not fresh, otherwise computes $K_1^* = h(PW_A \| ID_T)$ and decrypts E_1 with K_1^* as $(ag, W_1, C_A) = D_{K_1^*}(E_1)$. Computes $W_1^* = h(ID_A \| C_A \| ID_T)$ and verifies $W_1^* ?= W_1$. If yes, then generates $b \in Z_q^*$ and computes session key as $SK_T = h(ID_A \| ID_T \| C_A \| C_T \| bag \| t_3)$. Further, AV computes $W_2 = h(C_A \| C_T \| t_3)\ and\ K_2 = h(C_A \| ID_T)$. Finally, $iTwin$ encrypts $E_2 = E_{K_2}(W_2, bg, t_3)$ and sends $M_2 = \{E_2, t_3\}$ to AV.

Step 3. On receiving $M_2 = \{E_2, t_3\}$, *AV* first verifies $t_3 - t_2 \leq \triangle t$ if yes then computes the key $K_2^* = h(C_A \| ID_T)$ and decrypts $(W_2, bg, t_3) = D_{K_2^*}(E_2)$ with K_2^*. AV also computes $W_2^* = h(C_A \| C_T \| t_3)$ and verifies $W_2^* ?= W_2$. If yes then, *AV* computes the session key $SK_A = h(ID_A \| ID_T \| C_A \| C_T \| bag \| t_3)$. Finally, *AV* verifies the session key $SK = SK_A = SK_T$.

5. Security Analysis

This section offers a thorough examination of the suggested protocol's security features. We have carried out both official and informal evaluations to guarantee its resilience against prospective dangers. The privacy and secure verification of the AV and $iTwin$ participants are effectively guaranteed by the protocol. The following subsections contain our discussion of the security factors and findings:

5.1. Private Key Security

A private key k is selected by the user from the set of nonzero integers modulo q, as $k \in Z_q^*$ The associated public key P_{pub} is then determined by multiplying k by the generator g of the group G, as $P_{pub} = k.g$. In order for an attacker A to undermine the system's security, they would have to compute the private key using data that is accessible to the general public. But because the private key is derived using a master key g, and because the ECC

discrete logarithm issue is hard to solve, it becomes very hard for an attacker to figure out the private key. Due to the attacker's inevitable failure to breach the system, we can therefore state with confidence that its security is still intact.

5.2. Impersonation Attack

An impersonation attack is when a perpetrator poses as an authorized user with the intention of obtaining data or gaining an advantage. The information transmitted during the secret key establishment step must be used by the attacker to demonstrate their validity in order to successfully execute such an attack. We examine two categories of assaults including impersonation:

-**Autonomous Vehicle:** Here, in an attempt to obtain information or gain an advantage, the aggressor impersonates the AV organization. When creating a secret key, the AV uses a public channel to deliver $M_1 = \{E_1, t_1\}$ to the $iTwin$. It is nearly impossible for an attacker to determine E_1 or the private key due to the use of encryption with a private key and the ECC discrete logarithm problem. The attacker's attempt to pass for a legitimate AV entity will thus be futile.

– **iTwin-IA:** Here, by using the data that was shared during the secret key establishment process, the attacker tries to pass for a real iTwin entity. Both the $iTwin$ and the AV send out messages $M_1 = \{E_1, t_1\}$ and $M_2 = \{E_2, t_2\}$ across a public channel during this phase. However, computational constraints resulting from the ECC discrete logarithm problem make it exceedingly difficult for the attacker to calculate the secret keys K_1 and K_2 . As a result, the attacker will be unable to pass for an authentic $iTwin$ entity.

5.3. Mutual Authentication

Three entities are involved in the secret key establishment phase of the proposed protocol: $iTwin, C_A$, and AV. Every $iTwin$ and every AV node computes a shared key during the registration phase. They have to authenticate one another first, though, to confirm that their identities are real, before they can accept the shared key. Moreover, before moving forward to the following phases of the secret key agreement phase, all three parties participate in authentication, guaranteeing the confirmation of personal identification. Mutual authentication is therefore a crucial component of the system.

5.4. Session Key Disclosure Attack

Under the suggested protocol, $iTwin$ and AV calculate a secret key during the SK agreement stage. After that, the session key SK_A is computed using this key. It should be noted that all other parameters required to determine the session key are openly available, with the exception of a and b. Both $iTwin$ and AV have the identical randomly generated values for a and b. In polynomial time, an attacker would not be able to collect random information necessary to ascertain the values of a and b. Consequently, even if the attacker has the secret key K_1 or K_2, they are unable to derive the session key SK_T. Additionally, the suggested protocol uses a hash function to guarantee secure communication; since there are no invertible hash functions, the attacker cannot extract SK from the protocol description. As a result, the suggested protocol is safe from attacks that disclose session keys.

5.5. Eavesdropping Attack

The ability to intercept communications sent across an unprotected channel and disrupt communication is what defines an eavesdropping attack. In order to solve this issue, our suggested protocol generates a new random number for every authentication cycle and uses a hash function to calculate all other parameters. By using this method, the attacker cannot get any parameters or user ID_s . Moreover, the attacker cannot calculate the session key SK, therefore $ID_T, ID_A, C_A, E_1, E_2$ or SK_i cannot be obtained. As a result, the security of our suggested approach against listening in is strong.

5.6. Key Freshness

The freshness of the key is essential to preserving the communication channel's security. It is essential to produce a fresh key whenever the compromised one is compromised in order to prevent future connectivity from being distorted. We address this problem in our suggested method by selecting a new random integer and timestamp at each authentication stage to guarantee key freshness.

5.7.Perfect Forward Secrecy

In order to prevent an attacker from deriving the session key $SK = SK_A = SK_T$, the proposed protocol includes PFS. This is because there is no information about the previous key in the session key. It will also be difficult for the attacker to compute the new random numbers selected by both $iTwin$ and AV, which will render retrieving the value of abg or bag computationally impossible. Thus, even in the event that the private secret key is discovered, the protocol ensures perfect forward secrecy, preventing the compromise of session keys.

5.8.Replay Attack

The suggested protocol includes safeguards against replay attacks, in which a malevolent adversary tries to relay a message that has already been intercepted. The protocol uses the following countermeasures to stop such attacks: it uses a secure hash function, verifies conditions W_1 and W_2 and uses new timestamps and random integers. The suggested protocol is resistant to replay attacks because to these safeguards, which guarantee that any attempt to repeat a previously intercepted message would be unsuccessful.

5.9.Denial of Service Attack

To mitigate Denial of Service (DoS) attacks, the proposed protocol incorporates a safeguard mechanism that sets a maximum limit of three login/authentication attempts. The login and authentication features of an Autonomous Vehicle (*AV*) will be momentarily disabled if it does not successfully give the necessary credentials after three attempts. This restriction ensures that the system is always accessible and functional and successfully defends against denial-of-service (DoS) assaults.

5.10 .Offline User Identity Prediction Attack

An adversary's attempt to determine a user's identification by examining messages sent over an open channel is known as an offline user identity prediction attack. The suggested approach uses the user's identifier $ID_A$to generate a highly resistant password and private key in order to thwart this attack. By taking this precaution, the recommended system's resistance against offline user identity prediction attacks is greatly increased.

5.11 Autonomous Vehicle and iTwin Node Traceability Attack

In the autonomous vehicle and iTwin node traceability attack, the attacker attempts to locate the AV and $iTwin$ by tracking authentication communications. Using encrypted parameters E_1 and E_2 in conjunction with a one-way hash function, a private key, and a new timestamp, the suggested protocol counteracts this attack. Our plan guarantees that the AV and $iTwin$'s identities be kept secret, thwarting attempts to render the system untraceable.

5.12 Insider Attack

An insider attack is a hostile conduct in which a non-authorized user obtains access to a system and uses it to get passwords or other user data in order to attempt unauthorized logins to various services. The communications trans- mitted between *AV* and *iTwin* are encrypted using private keys, which are safely stored and available to authorized users only, to counteract this kind of assault. The technique effectively prevents unauthorized users from using com- promised identities to obtain sensitive information by putting this protection in place. As a result, the recommended architecture offers strong defence against insider threats.

5.12. Man in the Middle Attack

During login, an attacker can use past messages sent from the server side in a form of attack known as Man in the Middle Attack . Using new random numbers and pseudonymous identities, the proposed approach stops this attack by preventing the attacker from computing with the real entity. The suggested framework is also immune to this attack because the messages M_1 and M_2 are encrypted using private keys and secret keys, respectively, and are hidden by a hash function.

6. Performance analysis

We conducted extensive testing of our proposed protocol, comparing it with other relevant schemes proposed by Yao et al. [1], Wu et al. [2], Kumar et al. [3], and Nandy et al. [4]. We also analyzed and demonstrated the variations in key performance metrics, such as communication cost and computation cost. The evaluations were carried out on an Intel Pentium® CPU 2020 Model operating at 240 GHz and a 64-bit core Ubuntu 18.04 OS. Similar to the previous protocols, our suggested protocols were implemented using Python 3.6, a robust programming language. We utilized the popular network simulator (NS3) platform to test the proposed authentication protocol. In the subsequent subsections, we provide a detailed analysis of the performance and quantitative results obtained for each protocol.

6.1. Computation cost

For a comprehensive evaluation, we compared the computing costs in detail between our proposed methodology and those in earlier publications. To represent the times for carrying out different operations in our analysis, we used the symbols $t\_h, t\_ecm, t\_sym, and\ t\_fe$. These processes consist of using $SHA2$ to perform a unidirectional hash, multiplying points in elliptic curve cryptography, operating on symmetric keys in cryptography, and performing fuzzy extractor operations, in that order. Previous research [15] has shown that the computation times for fuzzy extractor and EC point multiplication are almost the same. The xor operation's execution time was configurable, thus it was left out of the computation. But these were the precise execution timings that were found: $t_h = 0.01975\ ms$, $t_{ecm} = 0.103156\ ms$, $t_{sym} = 0.063332\ ms$, and $t_{fe} = 0.103156\ ms$.

We restrict our calculation comparison to the authentication and communication steps because a vehicle can only be registered once. According to our research, the technique recommended by Wu et al. [2] calls for $34t_h$ + 2 t_{ecm} = 0.877812 ms, but Yao et al. [1] call for 22nd + 7 t_{sym} + 4 t_{ecm} = 1.290448 ms. Kumar et al. [3] also achieve execution time of $10t_h$ + 5 t_{ecm} = 0.69353 ms. Nandy et al. [4] state that the need is $13t_h$ + 2 t_{sym} + $1t_{fe}$ = 0.48657 ms. But, during operation, our proposed method only requires $11t_h$ + 4 t_{sym} = 0.470578 ms. We are able to determine from these comparisons that our proposed protocol has a superior computing efficiency.

6.2. Communication cost

The size of the messages that are sent back and forth at various protocol stages can be used to calculate the communication cost. The purpose of this section is to evaluate and compare the suggested protocols'

communication costs to those of earlier methods. We use the published work [15] for the communication parameter outcome. The expenses corresponding to each function and variable are shown separately. Four bytes specifically indicate a random nonce, eight bytes constitute a time stamp, and sixteen bytes represent an identity number. We use an ECC symmetric key of 16 bytes and the $SHA2$ one-way hash technique with a message digest size of 32 bytes for our protocol. The elliptic curve scalar multiplication, which yields a 20-byte representation, has been shown to be valid by earlier studies. In our suggested protocols, two messages are sent during the communication phase: $M_1 = \{E_1, T_1\}$ is a communication request from AV to $iTwin$, and $M_2 = \{E_2, T_2\}$ is a communication response from $iTwin$ to AV. 24 bytes (16 bytes + 8 bytes) are needed for each of these messages. At a total communication cost of 48 bytes, our protocol is hence. With regard to digital $iTwin$ communication systems, this feature renders the suggested protocol extremely appropriate and offers the best possible outcome.

7. Conclusion

We describe a vehicular digital twin-based system in this paper for computation and data integration in autonomous vehicles (AV). Our method involves synchronizing the digital twin with the physical vehicle, which collects the required data, and using the digital twin to do cloud computing in real-time and provide feedback. To ensure security, we provide verification protocols for communication both inside and between twins. Through security studies, we demonstrate our proposed approach's resilience against various forms of attacks. Furthermore, by contrasting the performance of our proposed method with existing ad hoc vehicular communication schemes, we demonstrate the greater reliability and efficiency of our methodology. The security analysis and performance evaluation demonstrate that our suggested protocol meets basic security criteria while lowering computer costs. Therefore, applying our proposed approach to scenarios involving digital twins is quite suitable.

References

[1] L. Yao, C. Lin, J. Deng, F. Deng, J. Miao, K. Yim, G. Wu, Biometrics-based data link layer anonymous authentication in vanets, in: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2013, pp. 182–187.

[2] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, Z. Zhu, An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network, IEEE Access 7 (2019) 55050–55063.

[3] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, M. K. Khan, RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing, Vehicular Communications 22 (2020) 100213.

[4] T. Nandy, M. Y. I. Idris, R. M. Noor, A. K. Das, X. Li, N. A. Ghani, S. Bhattacharyya, An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network, Computer Communications 177 (2021) 57–76.

[5] T. Zhang, X. Liu, Z. Luo, F. Dong, Y. Jiang, Time series behavior modeling with digital twin for internet of vehicles (2019).

[6] G. Bhatti, H. Mohan, R. R. Singh, Towards the future of smart electric vehicles: Digital twin technology, Renewable and Sustainable Energy Reviews 141 (2021) 110801.

[7] B. Alaya, L. Sellami, Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks, Journal of Information Security and Applications 58 (2021) 102779.

[8] M. La Manna, L. Treccozzi, P. Perazzo, S. Saponara, G. Dini, Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update, Sensors 21 (2) (2021) 515. URL https://www.mdpi.com/1424-8220/21/2/515

[9] Muniandi, B., Huang, C., Kuo, C., Yang, T., Chen, K., Lin, Y., Lin, S., & Tsai, T. (2019). A 97% maximum efficiency fully automated control turbo boost topology for battery chargers. IEEE Transactions on Circuits and Systems I-regular Papers, 66(11), 4516–4527. https://doi.org/10.1109/tcsi.2019.2925374

[10] J. Xu, C. He, T. H. Luan, Efficient authentication for vehicular digital twin communications, in: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), IEEE, 2021, pp. 1–5.

[11] D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on information theory 29 (2) (1983) 198–208.

[12] R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 337–351.

[13] S. Itoo, M. Ahmad, V. Kumar, A. Alkhayyat, RKMIS: robust key management protocol for industrial sensor network system, The Journal of Supercomputing (2023) 1–29.
[14] V. Kumar, A. M. A. Al-Tameemi, A. Kumari, M. Ahmad, M. W. Falah, A. A. Abd El-Latif, PSEBVC: Provably secure ecc and biometric based authentication framework using smartphone for vehicular cloud environment, IEEE Access 10 (2022) 84776–84789.
[15] V. Kumar, RSFVC: Robust biometric-based secure framework for vehicular cloud networking, IEEE Transactions on Intelligent Trans- portation Systems, IEEE, 2023.
[16] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, Design of secure key management and user authentication scheme for fog computing services, Future Generation Computer Systems 91 (2019) 475–492.
[17] K. Kumar, V. Kumar, Seema, Robust Authentication Protocol for Autonomous Vehicle using Digital Twin Networks, Tuijin Jishu/Journal of Propulsion Technology, 2632 – 2645, 45(1), 2024.