# A Secure Authentication Method Based On Digital Twins For Vehicle Cloud Networking

Dheeraj Tiger[1] , Nishu[2] , Vinod Kumar[*3] , Anshu Malhotra[4]

[1]Department of Applied Sciences, The North cap University, Gurugram-122017, India.
Email: dheerajtiger@gmail.com, India
[2]Department of Computer Science and Engineering, The North Cap University, Gurugram-122017, India. Email: sethinishu@gmail.com
[3]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi-110032, India.
Email: vinod.iitkgp13@gmail.com & vkmaths@shyamlal.du.ac.in
[4]Department of Computer Science and Engineering, K R Mangalam University Gurugram-122103, India. Email: anshu@krmangalam.edu.in
*: Corresponding author

**Abstract:** Autonomous vehicles (AVs) provide various services but are usually plagued with sensing, processing, and communication delay issues. To mitigate these challenges, we introduce a secure cloud-based digital twin framework that allows real-time synchronization and data fusion with physical vehicles. This solution minimizes communication overhead, enhances system responsiveness in general, and promotes a better passenger experience. In addition, it provides data security and privacy during the interaction process. In comparison to other vehicular communication protocols, our approach is less computationally intensive and thus extremely appropriate for real-time applications. The system is intended to allow secure and efficient data transfer from the vehicle and its digital twin without impairing performance. Optimizing communication and computation equally, our solution offers a scalable platform for autonomous vehicle deployments in the future. In general, this work is a milestone toward the integration of digital twin technology with AV systems in a seamless and secure manner.

**Keywords:** Autonomous vehicle, Digital twin, ECC, Security and Privacy.

## 1. Introduction

Autonomous vehicle research has experienced significant progress in recent past years, both in industry and academia. Large automotive manufacturers such as Tesla, Volvo, and Toyota have invested heavily in the production of autonomous vehicles (AVs). Consequently, numerous new car models now include Level 2 autonomy, where the vehicle can control steering, acceleration, and braking in specific conditions. AVs are preloaded with sensors and computing modules, serving as mobile computing platforms. These are systems that are able to detect and react to environmental factors like traffic lights, roadblocks, pedestrians, and weather. The data is utilized by AVs to make immediate decisions regarding speed and direction in order to travel safely and comfortably. Real-time sensing, processing, and communication, however, put huge burdens on a vehicle's onboard resources. This has the potential to cause performance problems, e.g., delay or corruption of processing, which can undermine safety or cause an inferior passenger experience. Moreover, the communication radius of an AV is by nature limited, rendering it unable to sense traffic conditions or dangers outside its surrounding vicinity. In response to these issues, we introduce in this setting a newly authentication framework. This solution improves AV performance by allowing secure, real-time synchronization and data exchange with cloud-hosted digital twins. With this framework, AVs can access more comprehensive environmental and traffic data, enhancing decision-making and minimizing onboard computational resources. In the end, our method reinforces data fusion, enhances safety, and maximizes overall driving experience in autonomous vehicle systems.

We introduce a novel online virtual vehicle model, called iTwin, that serves as the digital twin (DT) of its actual world autonomous vehicle (AV), as shown in Fig. 1. The iTwin captures important information from its associated AV, such as favorite routes, destination history, local road knowledge, and personal driving habits. In order to lighten the computational burden on the physical AV, real-time decision-making and processing are transferred to the cloud through the use of iTwin. The processed output is sent back to the vehicle, allowing for effective and responsive driving operations. The iTwin architecture also makes it possible to share data among digital twins of multiple AVs. This allows the iTwins to share important road and traffic information and pass it on to their respective physical AVs. Such cross-vehicle digital twin communication significantly enhances the awareness of the AV beyond its short-range sensing capability—from line-of-sight to even city-wide in vision—without incurring extra infrastructure or expense. This iTwin-informed framework not only alleviates the computational burden on AVs but also greatly improves their capability of making safer and wiser driving decisions. It facilitates improved route planning, hazard detection, and responsive behavior in a changing world. Through the use of digital twin technology, our system enhances passenger safety and user experience. Our belief is that this methodology can help drive autonomous vehicle development and real-world deployment forward, providing a scalable and smart solution to numerous challenges facing the field today.

### 1.1 Related work

The progress of the Internet of Vehicles (IoV) has been pushed much further by combining Digital Twin (DT) technology with the Internet of Things (IoT). This integration enables effective, real-time sharing of data between different entities in the vehicle network. For example, Zhang et al. [5] demonstrated mobile Electric Vehicles (EVs) as mobile charging stations using mobility models with DTs to evaluate multiple IoV navigation approaches. Likewise, Bhatti et al. [6] proposed a complex EV DT system to support the improvement of transportation management in the IoV system. Notwithstanding these innovations, IoV is confronted with imperative security issues. Data confidentiality and integrity may be lost through malicious intermediaries during transmission between IoV nodes. Symmetric algorithms such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are typically used because of their high speed and low computational overhead, which is ideal for encrypting real-time, high-volume data. Asymmetric encryption techniques such as Elliptic Curve Cryptography (ECC) and ElGamal provide increased security using public key infrastructure, keeping only the private key on each node. Sellami and Alaya [7] enhanced data rates of transmission in Ad Hoc Vehicular Networks with a hybrid key management scheme. La Manna et al. [8] enhanced automotive security with attribute-based encryption for wireless updates. Xu et al. [9] introduced a bilinear mapping-based authentication scheme for vehicular DT communication. Still, a systematic DT modelling approach dedicated to IoV and Cyber-Physical Systems is less explored. To meet this challenge, our research suggests a focused DT modelling approach and an effective asymmetric encryption-based security mechanism. This method optimizes data safety and reduces encryption and decryption delay, thus enhancing the overall performance and safety of vehicular DT communication in the IoV environment.

### 1.2. The paper structure

The paper's structure includes Section 2 on the proposed iTwin communication model, Section 3 describes mathematical preliminaries, Section 4 on authentication and key agreement phase, and Section 5 on security analysis. Section 6 presents performance evaluation and concludes with future directions and a summary of key contributions.

## 2. System Model

Autonomous vehicles (AVs), a central authority (CA), and related cloud-based iTwins compose the system model of our proposed vehicle digital twin communication architecture, as illustrated in Fig. 1. Notable characteristics of each stakeholder and their security needs are outlined in the subsequent details:

- **Central Authority (CA):** The CA is tasked with generating secret keys and pseudonyms for each AV and iTwin in the system. Additionally, it is tasked with issuing each iTwin a group certificate permitting communication with other iTwins upon successful AV authentication. In

the event of malfunctioning messages or security breaches, the CA should be able to detect and track the legitimate identities generated by iTwins.

- **Autonomous Vehicle (AV)**: In order to enhance the level of service, the AV talks to all iTwin and gathers data from its inbuilt sensors. It needs to authenticate itself with the CA before getting into communication with any iTwin and confirming secure communication channels so that it can safeguard the confidentiality and integrity of information it transmits.
- **iTwin**: To improve the overall happiness of passengers, the iTwin provides computational services using data gathered from its connected physical vehicle. To safeguard the integrity and confidentiality of the received and transmitted data; it must authenticate itself with the CA prior to establishing a secure communication channel with the AV.


**Figure 1: System model**

We need to have secure authentication and communication among all concerned in an effort to provide security to the said framework. For each AV and iTwin, the CA will have to produce strong pseudonyms and secret keys in an effort to thwart impersonation attacks. Depending on the urgency and sensitivity level of the information, all communication channels between the AV, iTwin, and CA must be encrypted using symmetric or asymmetric encryption algorithms. Furthermore, to avoid any security breach or miscommunication, the CA should be able to monitor genuine identities formed by iTwins. The confidentiality and integrity of data transfer in our vehicle digital twin communication system can be maintained by putting these security controls in place.

**Table 1: Notation and their meaning**

| Symbol | Meaning | Symbol | Meaning |
|---|---|---|---|
| EC | Elliptic curve | S K | 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 |

### 2.1. Attacker Model

Considering the high-risk nature of Digital Twin (DT) networks, it is important to thoroughly investigate possible security weaknesses. In this research, the Dolev-Yao (DY) threat model [10] is employed to analyze mutual authentication and session key negotiation procedures. The DY model supposes that a malicious attacker can intercept, alter, and create messages but not compromise cryptographic primitives. For additional reliability in the security analysis, the Canetti-Krawczyk (CK) adversary model [11] is also employed. The CKM model upgrades the DY model by enabling the attackers to acquire session-specific temporary credentials that may ultimately result in a compromise of session keys agreed upon. This wider scope gives a better and more realistic assessment of the capabilities of an attacker and potential threats in the system. By using both the DY and CKM models, the present study presents an extensive evaluation of the mutual authentication and session key negotiation process in DT

networks. The use of both models provides a strong testing against a variety of adversarial attacks, making the suggested communication protocol more reliable and secure in the DT setting.

## 3. Mathematical Preliminaries

In this section, we lay out the mathematical methods and terminology required to adequately analyze and describe the proposed framework.

### 3.1 Notation

Table 1 lists the significant notation used in the suggested framework.

### 3.2 Background of ECC

Elliptic Curve Cryptography (ECC) is a robust public key cryptographic technique based on the mathematics of large finite field elliptic curves. While conventional public key methods like RSA use larger key sizes to attain similar or greater security, ECC achieves similar or better security levels with much smaller key sizes. This makes ECC highly appealing for systems that have few computational resources available, like mobile phones and embedded systems. The smaller key size, in addition to enhancing processing speed, also reduces storage and transmission needs, thereby generally increasing performance. ECC is now a top pick in securing data in contemporary digital communications, providing robust encryption with low overhead. Research has established that ECC is efficient in protecting data against attacks in cryptography without sacrificing efficiency, thereby being appropriate for high-performance as well as resource-constrained systems. Because of its relative security and computational benefits, ECC is very much used in today's cryptographic standards and protocols for encrypting digital data[12, 13]. Let us consider a prime number q of noteworthy magnitudes, and $a, b \in Z_q^*$, where $Z_q^*$ is a finite field. Supposing $4a^3 + 27b^2 \neq 0 \pmod q$, we may construct a non-singular elliptic curve $E_q(a, b)$ over the finite field $Z_q^*$with the equation:

$$E_q(a, b) : y^2 \equiv x^3 + ax + b \bmod q$$

The additive group G of the elliptic curve is given by $G = \{(x, y): x, y \in Z_q^*, (x, y) \in E_q\} \cup \{\Theta\}$. As the same element (zero element) within $G, \Theta$ represents the asymptotic point here. The group operations on the group $G'$ are as follows [14]:

- **Scalar Multiplication:** Let P be the elliptic curve's base point $E_q(a, b)$. The definition of the scalar multiplication operation is:
  $k \cdot P = P + P + \ldots + P$ (k times), where $k \in Z_q^*$ is a positive integer.
- **Point Addition:** For $P = (x_1, y_1)$, $Q = (x_2, y_2) \in G$, the addition of P and Q is denoted as $P + Q = (x_3, y_3)$, where: $x_3 = \ell_2 - x_1 - x_2 \pmod q$ and $y_3 = (\ell(x_1 - x_3) - y_1) \pmod q$ and $\ell$ is defined as:
  $$\ell = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \bmod q \text{ if } P \neq Q \\ \frac{3x^2 + a}{2y_1} & \bmod q \quad \text{if } P = Q \end{cases}$$
- **Point Negation:** The negation of $P = (x, y) \in G$ is $-P = (x, -y)$.

## 4. The proposed protocol

The following stages are included in the suggested protocol:

### 4.1 Initialization phase

CA can play the role of a third party or a public/private key generator. During the initialization phase, the following actions are taken:

- Based on $E_q(a, b): y^2 = x^3 + ax + b \pmod q$, CA selects the non-singular EC.
- g is chosen as G's group generator. The public key $PK_C = cg$ is set, and the secret key for CA, $c \in Z_q^*$, is chosen at random. selects the secure hash function.
- In order to determine the public key, AV computes $PK_A = ag$ and selects $a \in Z_q^*$ as the private key.
- $PK_{iT} = kg$ is the public key that iTwin sets after selecting a random number $k \in Z_q^*$ as the private key.

### 4.2. Registration phase

Through the CA, AV and iTwin must register in order to receive the data required for communication with the DT-vehicular network. It is essential that AV, iTwin, and CA come to an agreement. Here is a thorough explanation of the AV and iTwin registration process:

**Step 1:** Firstly, AV enters his identity $ID_A$ and password $PW_A$, calculates $J_{R1} = h(PW_A \| ID_A)$, and transmits $\{ID_A, PW_A, J_{R1}\}$ to CA over a secure channel.

**Step 2:** After obtaining the aforementioned data, CA produces $C_T \in Z_q^*$. Following that, CA sends $\{ID_A, PW_A, J_{R1}, C\}$ for iTwin via secure.

**Step 3:** After obtaining the aforementioned message, iTwin enters its own identification $ID_T$ . It then calculates $J_{R2} = J_{R1} \oplus h(ID_T \| ID_A)$ and transmits $\{J_{R2}, ID_T\}$ to CA using a secure channel.

**Step 4:** After iTwin sends the aforementioned communication, CA creates $C_A \in Z_q^*$ and sends $\{H_{R2}, ID_T\}$ to AV after that.

**Step 5:** After AV receives $\{HR_2, C_A\}$, it calculates $J_{R3} = J_{R2} \oplus h(ID_T \| ID_A)$. AV finally saves $J_{R3}$ in a database.

### 4.3. Login and authentication phase

AV and iTwin authenticated against each other during registration to create a shared session key. The details of the authentication and login process are as follows:

**Step 1.** AV login with identity $ID_A^*$ and password $PW_A^*$ and computes $J_{R1}^* = h(PW_A^* \| ID_A^*)$. AV verifies $J_{R3} ?= J_{R1}^*$ if yes then AV generates a $\in Z_q^*$. AV computes $J_1 = h(ID_A \| C_A \| ID_T)$ and $K_1 = h(PW_A \| ID_T)$. Then, AV encrypts $(ag, J_1, C_A)$ with $K_1$ as $E_1 = E_{K1}(ag, J_1, C_A)$. 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 $(ag, W_1, C_A) = D_{K_1^*}(E_1)$. Further, iTwin Computes $J_1^* = h(ID_A \| C_A \| ID_T)$ and verifies $J_1^* ?= J_1$. If yes, then generates $b \in Z_q^*$ and computes session key as $SK_T = h(ID_A \| ID_T \| C_A \| C_T \| bag \| t_3)$. Furthermore, AV computes $J_2 = h(C_A \| C_T \| t_3)$ and $K_2 = h(C_A \| ID_T)$. Finally, iTwin encrypts $E_2 = E_{K2}(J_2, bg, t_3)$ 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 $(J_2, bg, t_3) = D_{K_2^*}(E_2)$ with $K_2^*$. AV also computes $J_2^* = h(C_A \| C_T \| t_3)$ and verifies $J_2^* ?= J_2$. 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 $SK = S K_A = S K_T$.

## 5. Security Analysis

This section provides an in-depth examination of the security aspects of the proposed protocol. Formal and informal evaluation techniques have been utilized to determine its resilience towards diverse security attacks. These analyses serve to establish the strength of the protocol and its ability to preserve data integrity and confidentiality. Particular focus has been given to the privacy and secure authentication of Autonomous Vehicles (AVs) and iTwin entities in communication. The protocol ensures resistance to attacks, protects sensitive data, and ensures trust between participating entities. By exhaustive testing and validation, the system has proved robust defense mechanisms to counter known attacks. The privacy-preserving techniques that are incorporated in the protocol guarantee identity and data protection along the interaction process. Comprehensive security evaluations, including their results, are presented in subsequent subsections, which identify the protocol's robustness and efficiency in ensuring secure operation over the vehicular cloud computing environment:

### 5.1. Impersonation Attack

An impersonation attack happens when the attacker pretends to be an authorized user in order to get unauthorized access to data or services. To conduct the attack successfully, the attacker has to take advantage of information shared during the secret key establishment phase to present oneself as valid. It mostly happens when the attacker intercepts or tampers with authentication data in order to mislead the system. Secure key exchange is thus essential to avoid such attacks. Here, we study two particular forms of impersonation attacks, discussing how they work and assessing the resilience of the protocol against them through solid cryptographic techniques and safe authentication practices.

- **Autonomous Vehicle:** In this case, the adversary tries to masquerade as the AV firm for information gathering or to gain an upper hand. At secret key generation time, the AV broadcasts $M_1 = \{E_1, t_1\}$ to the iTwin through an open channel. Nevertheless, with the employment of encryption using a private key and the difficulty of the ECDLP, it is computationally impracticable for the attacker to acquire $E_1$ or the private key. Consequently, the attacker's attempt to impersonate a genuine AV entity fails, protecting the system from successful impersonation attacks.
- **iTwin-:** In such a situation, the attacker tries to masquerade as a valid iTwin entity using information shared in the secret key establishment process. Here, the AV and the iTwin talk to each other in terms of messages $M_1 = \{E_1, t_1\}$ and $M_2 = \{E_2, t_2\}$, sent through an open channel. In order to impersonate the iTwin successfully, the attacker must calculate the secret keys $K_1$ and $K_2$ from this shared data. Thanks to the sound computational security ensured by the ECDLP, it is theoretically impossible for the attacker to know these secret keys. The ECDLP guarantees that the private key cannot be derived from the public key even with complete access to transmitted messages. Therefore, the attacker's attempt at impersonating an original iTwin entity will always fail, maintaining integrity and authenticity of the communication. entity.

**5.2. Private Key Security**

In ECC, a user picks the private key k from the set of nonzero integers modulo q, i.e., $k \in Z_q^*$. The resultant public key $P_{pub}$ is obtained by taking the product of the private key k with a publicly shared generator g of the elliptic curve group G, i.e., $P_{pub}$ =kg. For an attacker to compromise the system, he must calculate the private key from the public key and the generator, both of which are publicly known. This computation, though, is computationally infeasible because of the intractability of the ECDLP. This mathematical problem is the basis of the security of ECC. Consequently, even if an attacker knows $P_{pub}$ and g, he cannot practically calculate k. Hence, the system is still secure, and its cryptographic strength is ensured with confidence.

**5.3. Session Key Disclosure Attack**

In the suggested protocol, iTwin and AV jointly compute a secret key in the session key (SK) agreement process. On this basis, a session key $SK_A$ is computed. Importantly, all parameters that are needed to calculate the session key are known openly, apart from two significant values, a and b, which are chosen at random and shared confidentially between iTwin and AV. These values are not known to any third party. Because a and b are random and secret, it is infeasible for an attacker to find them within polynomial time. Even if the attacker succeeds in obtaining either of the secret keys $K_1$ or $K_2$, they cannot still calculate the session key $SK_T$ without being aware of a and b. Further, the implementation of a cryptographic hash function also provides additional security because hash functions are one-way and non-invertible. Thus, the protocol securely protects against session key disclosure attacks.

**5.4. Mutual Authentication**

In the secret key setup phase of the proposed protocol, three entities are involved: iTwin, CA and AV. During this phase, each iTwin and AV node generates a shared secret key at the time of registration. However, before establishing this shared key, it is essential that both entities authenticate one another to verify the legitimacy of their identities. This mutual authentication process ensures that only trusted parties can participate in the key agreement. Furthermore, all three entities- iTwin, CA, and AV-undergo an authentication step before advancing to the subsequent stages of the key agreement process. This additional layer of verification further strengthens the protocol's security and ensures that identity spoofing or unauthorized access is effectively prevented. Thus, mutual authentication is a critical component of the proposed system, playing a key role in maintaining secure and trustworthy communication between all participating entities.

**5.5. Key Freshness**

Key freshness is vital to ensure the security and integrity of a communication channel. The use of old or compromised keys can result in unauthorized access and data breach, and compromise all subsequent communications. It is hence very important to create a new key whenever there is a possibility of key compromise. For solving this, the given protocol guarantees key freshness with each authentication stage by adding a newly generated random integer and a fresh timestamp. This dynamic key material

generation assures that each session has a new, independent key, thus minimizing the possibility of replay or reuse attacks significantly. Adding a timestamp also enhances the process as it does not allow reuse of stale authentication data. This mechanism ensures that even if the previous key was compromised, it would have no impact on the security of subsequent sessions. Therefore, the suggested approach truly maintains secure, time-sensitive communication with robust key freshness principles.

**5.6. Eavesdropping Attack**

An eavesdropping attack involves intercepting communications transmitted over an open or insecure channel, with the intent to access sensitive information or disrupt communication. To counter this threat, the proposed protocol introduces a unique random number in each authentication round, ensuring that every session remains distinct and unpredictable. Additionally, the protocol utilizes secure hash functions to compute all relevant parameters, making it impossible for an attacker to reverse-engineer or extract any meaningful data. As a result, critical values such as user identities $(ID_S, ID_T, ID_A)$, cryptographic components $(C_A, E_1, E_2)$, and the session key $(SK_i)$ remain completely secure. Even with access to the communication channel, the attacker cannot compute or retrieve the session key $SK$. This combination of randomization and cryptographic hashing ensures that the protocol maintains strong resistance against eavesdropping attacks, thereby preserving the confidentiality and integrity of user communications.

**5.7. Replay Attack**

The protocol adopted in the proposed scheme has robust countermeasures against replay attacks, wherein an evil-minded attacker attempts to resend old captured messages to mislead the system. The protocol achieves this in order to avoid such attacks by having multiple countermeasures. It applies a secure cryptographic hash algorithm that guarantees data integrity and authenticity. Besides this, it evaluates certain conditions $H_1$ and $H_2$, which ensure the freshness and accuracy of the data being exchanged. Above all, the protocol produces a fresh timestamp and a random number for every authentication session. The dynamic values prevent any single session from being repeated. Due to these combined security features, any effort on the part of an intruder to replay a message that has been previously captured will be identified and refused. Therefore, the suggested protocol efficiently guarantees resistance against replay attacks and protects the communication process from repetition-of-messages-based attacks.

**5.8.Perfect Forward Secrecy**

To guarantee that an attacker will be unable to infer the session key $SK = SK_A = SK_T$, Perfect Forward Secrecy (PFS) is implemented in the proposed protocol. PFS guarantees session keys to remain secure even when long-term private keys are subsequently compromised. It does this by structuring the session key so that it includes no information connecting it to earlier keys or sessions. In both the authentication phases, the $iTwin\ and\ AV$ both generate new random numbers independently. These are utilized in calculating the session key but are never used again, and hence it becomes computationally infeasible for the attacker to build up the shared secret or calculate abg or bag. Since these random numbers and calculations are session-specific and not stored, even if the private key is compromised, past and future session keys are still secure. Therefore, the proposed protocol securely provides Perfect Forward Secrecy and enhances overall communication security.

**5.9. Denial of Service Attack**

For Denial of Service (DoS) protection, the suggested protocol includes a security function that restricts attempts at login or authentication. In particular, $AV$ has only three attempts to present legitimate credentials when authenticating. If the $AV$ is unable to authenticate within the three attempts, its login and authentication functionality is temporarily disabled. This precaution shields the system from being overwhelmed with constant invalid login requests by an attacker, something that would otherwise clog the server and interfere with normal operation. Through imposing this limitation, the protocol guarantees the system responds, is stable, and available to valid users. This process not only protects the system against DoS attacks but also enforces access control by identifying and rejecting repeated authentication failures. Consequently, the protocol proposed here ensures uniform service availability and enhances system-wide security against disruptively trying and unauthorized access.

**5.10 Insider Attack**

An insider attack is a malicious user who obtains unauthorized access to a system to steal passwords or sensitive user information and performs unauthorized logins on different services. To defend against this threat, the proposed protocol protects all communications between the $AV \ and \ the \ iTwin$ via private keys that are shared only among authorized parties. These private keys also guarantee that only authentic participants can decrypt and comprehend exchanged messages while blocking unauthorized access to sensitive information. By limiting access to the encryption keys and imposing strict identity authentication, the protocol successfully blocks attackers from using exploited identities. Consequently, sensitive information is safe, and unauthorized users cannot exploit internal system resources. By means of this security mechanism, the current proposal provides an effective defense against insider attacks, guaranteeing both confidentiality and integrity of communications between legitimate entities within the network.

**5.12. Man in the Middle Attack**

While logging in, an attacker who is Man-in-the-Middle might try to intercept and replay earlier messages from the server for impersonating legitimate parties. The suggested protocol secures effectively against such attacks through the use of new random numbers and pseudonymous identities within every session of authentication. These dynamic factors do not allow the attacker to trace intercepted messages to actual parties, making replay or impersonation efforts futile. Moreover, the authenticity messages $M_1 \ and \ M_2$ communicated during the authentication process are securely encrypted with private keys and session-specific secret keys, respectively. Additional protection comes in the form of masking these messages with a cryptographic hash function to ensure their integrity and confidentiality. This multilayered security measure makes it that even if communication is intercepted by an attacker, they will not be able to decipher or tamper with the information to gain unauthorized access. As such, the protocol is highly resistant against Man-in-the-Middle attacks during the login procedure.

**6. Performance analysis**

Comparing to past pertinent approaches provided by Yao et al. [1], Wu et al. [2], Kumar et al. [3], and Nandy et al. [4], we tested our proposed process extensively. Critical performance measures, like computation and communication expenditures, were analyzed and variations were exhibited. An Intel Pentium® CPU 2020 Model processor operating at 240 GHz and utilizing Ubuntu 18.04 with 64-bit cores was utilized for the simulations. We encoded our proposed protocols using Python 3.6, a powerful programming language, just like the earlier protocols. We employed the widely used network simulator (NS3) platform to conduct simulations for testing the proposed authentication protocol. We give a detailed description of the performance and numerical results attained for each protocol in the following subsections.

**6.1. Cost of computation**

In a detailed analysis, we have compared the computational expenditures of our new approach with that of previous research. Our work employed notations $t_h, t_{ecm}, t_{sym}$, and $t_{fe}$ to represent the timings for carrying out various operations. These are elliptic curve point multiplication, symmetric key cryptography operations, fuzzy extractor operations, and carrying out a one-way hash using SHA2, respectively. In earlier work [15], it was demonstrated that the execution times of fuzzy extractor and EC point multiplication are almost identical. Because the execution time of XOR operation can be modified, its execution time was not included in the calculation. But the actual execution times that were determined were the following: $t_h = 0.01975\, ms,\ t_{ecm} = 0.103156\, ms,\ t_{sym} = 0.063332\, ms, and\ t_{fe} = 0.103156\, ms$. Because an automobile can only be registered once, we limit our comparison of computations to the communication and authentication phases. From our research, Yao et al. [1] need $22t_h + 7\, t_{sym} + 4\, t_{ecm} = 1.290448\, ms$ and Wu et al. [2] suggest a solution that needs $34t_h + 2\, t_{ecm} = 0.877812\, ms$. Also, $10t_h + 5\, t_{ecm} = 0.69353\, ms$ is the execution time provided by Kumar et al. [3]. The required time is $13t_h + 2\, t_{sym} + 1t_{fe} = 0.48657$ ms according to Nandy et al. [4]. Our proposed method, however, needs only $11t_h + 4\, t_{sym} = 0.470578\, ms$ when in operation. These comparisons enable us to say our proposed protocol is more computing efficient.

### 6.2. Communication cost

The size of messages exchanged during different protocol phases can be utilized to determine the communication cost. We analyze and compare here the communication costs of proposed protocols with previous ones. For the result of the communication parameter, we refer to the existing literature [15]. The associated costs for each function and variable are displayed individually. A time stamp consists of eight bytes, an identifying number consists of sixteen bytes, and four bytes uniquely identify a random nonce. We utilize a 16-byte ECC symmetric key and the SHA2 one-way hash algorithm with a 32-byte message digest size within our protocol. It has already been shown by prior research that the elliptic curve scalar multiplication, a 20-byte representation, is valid. In our designed protocols, there are two messages that are exchanged during the communication phase: $M_1 = \{E_1, T_1\}$ is an AV-to-iTwin communication request, and $M_2 = \{E_2, T_2\}$ is an iTwin-to-AV communication response. 24 bytes (16 bytes + 8 bytes) are needed for both messages. With a communication cost of 48 bytes, our protocol is thus. When considering digital iTwin communication systems, the feature makes the proposed protocol very suitable and provides the optimal result.

## Conclusion

In this work, we introduce a vehicular digital twin-based system for computation and data integration in autonomous vehicles (AV). Our system synchronizes the digital twin with the real-world vehicle that collects the needed data in real-time. The digital twin is then used to conduct cloud-based computing to analyze this data and give timely feedback to the vehicle. In order to provide safe communication within one twin and among multiple twins, we provide strong verification protocols. Security evaluations prove that our suggested solution is strong against numerous forms of cyberattacks, maintaining data integrity and confidentiality. We also provide the performance comparison of our approach with conventional ad hoc vehicular communication protocols, specifying its higher reliability, effectiveness, and lower computation overhead. The collective results of the security test and performance testing reaffirm that our protocol is secure enough to meet basic security needs and conserves resources. Thus, our approach is very ideal for vehicular digital twin applications since it offers a safe and efficient system to optimize AV operation and communication.

## 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] 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.

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

[11] 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.

[12] 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.
[13] 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.
[14] V. Kumar, RSFVC: Robust biometric-based secure framework for vehicular cloud networking, IEEE Transactions on Intelligent Trans- portation Systems, IEEE, 2023.
[15] 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.