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

Robust Authentication Protocol for Autonomous Vehicle using Digital Twin Networks

Kamal Kumar[1], Vinod Kumar[2,*], Seema[1], Ramakant Prasad[3]
[1]*Department of Mathematics, Baba Mastnath University, Rohtak-124021, India;*
[2]*Department of Mathematics, Shyam Lal Collage, University of Delhi, New Delhi -110032, India;*
[3]*Department of Mathematics, Gargi Collage, University of Delhi, New Delhi-110049, India;*

Abstract: **-** In the modern world, vehicular networking is gaining tremendous importance. There are various challenges related to secure communication in vehicular networking. To address the security related concerns, digital twin technology provides a secure authentication framework and minimizes the risk of unauthorized access to the vehicular communication. By comparing the behaviour and characteristics of the physical device with its digital twin, authentication mechanisms can verify the authenticity of the device before granting access to specific services or resources. By implementing digital twin technology alongside authentication systems, it becomes possible to authenticate the identity of individuals interacting with industrial control systems or performing critical operations. The paper proposes a secure authentication protocol which satisfies the essential security standards as per the security analysis and performance evaluation. The paper also provides comparative analysis of the proposed framework with other peer frameworks in terms of computation and communication costs associated.

Keywords*: Digital Twin, ECC, Authentication, Security, Autonomous Vehicle*

1. Introduction

A virtual depiction of a real-world entity that can comprehend and anticipate its actual counterparts is known as "digital twin" as shown in Figure 1. A digital specification of its counterpart, data about that counterpart and an information model that connects and presents the data to support decision-making with each entity connected make up a digital twin [1]. Creating a digital thread by digital twins can facilitate data flows and offer an integrated view of asset data. Using AI, the simulation of a digital thread can reveal inefficiencies in operational efficiency and generate several chances for process optimization [2].

Fig. 1: Digital Twins

Digital twin technology can be applied in various areas like power generation equipment, heavy structures and systems, manufacturing hubs, healthcare, retail, automotive, disaster management, urban planning, smart cities, and a lot of other related areas. Digital twin technology offers the below advantages [3]:

- **Higher effectiveness**: Digital twins can aid in monitoring and mirroring production systems even after a new product has entered production, with the goal of reaching and maintaining peak efficiency throughout the whole manufacturing process.

- **Improved research and development**: Utilizing digital twins produces a wealth of data regarding expected performance results, facilitating more efficient product research and creation. Before beginning production, businesses can use this data to gain insights that will help them make the necessary product improvements.
- **Product life cycle:** Digital twins can also assist producers in determining how to manage products that have reached the end of their useful lives and require final processing, such as recycling or other actions. They can decide which product materials can be gathered by utilizing digital twins.

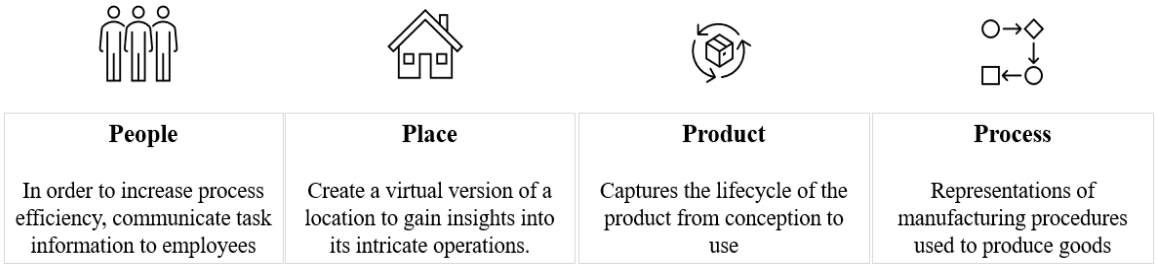

Fig. 2: Types of digital twins

Digital twins can be attributed to people, process, product, and process as shown in Figure 2 [4]. Digital twins are effective masterminds for boosting performance and innovation. Within the next five years, digital twins will represent billions of items. These substitutes for the physical world will create new chances for interaction between data scientists, whose job it is to comprehend what data tells us about operations and product specialists who specialize in the physical world. Using digital twin technology, businesses can better understand their customers' wants and create improvements for their current goods and services [5]. However, there are issues related to integration, cost, privacy, and security that need to be addressed [6].

1.1. Related peer work

In 1992, Horng et al. provided a scheme for authentication using a password table [7]. However, it was not a secure authentication framework as the message could be decrypted if anyone got access to the password table. Later in 1995, Yang et al. improved the authentication scheme using discrete logarithmic functions [8]. This scheme was quite related to the traditional schemes based on certificates. Later in 2002, Chien et al. provided a new authentication scheme using smart cards [9]. However, there were issues related to power and inflated costs associated with smart cards. In 2014, Nam et al. introduced an authentication scheme based on elliptic curve cryptography (ECC) for wireless networks [10]. However, the framework lacked user anonymity which leads to security issues. During the same year, Sangita et al. proposed a mobile cloud computing framework for authentication [11]. In 2015, Ling et al. proposed authentication based on one-time password for WSN (Wireless Sensor Networks) [12]. In 2016, Surekha et al. proposed Radio Frequency Identification (RFID) based authentication protocol [13]. In 2017, Tiwari et al. provided a lightweight scheme for IoT (Internet-of-Things) authentication [14]. In 2018, Megha et al. presented an authentication framework using smart cards in IoT environment [15]. In 2019, Ignacio et al. provided a multi-factor authentication framework [16]. In this year, Mohanaad et al. presented an authentication layer for public cloud computing [17]. In 2020, Latifa et al. proposed a novel authentication technique using cloud [18]. Later, Hasan et al. provided an enhanced authentication framework using cloud computing [19]. In 2021, Galal et al. proposed an authentication framework for bigdata [20]. In 2022, Ammar et al. proposed IoT protocol-based authentication framework [21]. Later, Samson et al. proposed an authentication framework for healthcare applications [22]. During the same year, Michal et al. presented authentication framework for Internet of Things [22]. In 2023, Abdul et al. proposed cloud Computing Authentication Frameworks [23]. During the same year, Rui et al. provided authentication framework for 5G technology [24].

1.2. Notations

The notations in the entire paper and their description are given in Table 1.

Table 1: Notations

Notation	Definition
EC	Elliptic curve
CA	Central Authority
AV	Autonomous Vehicles
iTwin	iTwin vehicular cloud
G	ECC based group
Id_i	The unique identity of i^{th} participant
Pw_i	Password of i^{th} identity
Sk_i	Session key of entity i
$\stackrel{?}{=}$	Whether equal or not
$\oplus$	Bitwise XOR operation
Z_q^*	Additive group of order q
$\|\|$	Concatenation operation
$\triangle T$	Valid time delay in message transmission
$\longrightarrow$	Public channel
$\Longrightarrow$	Secure Channel

1.3. Motivation

The motivation for this research paper stems from the need to design a robust authentication framework for vehicular networking that leverages digital twin technology. The proposed framework aims to overcome the limitations of traditional authentication mechanisms and provide enhanced security, privacy, and resilience in the face of various threats and dynamic network conditions. By incorporating digital twin technology, we can create virtual replicas of vehicles, capturing their characteristics, behaviour, and context. These digital twins can be used to establish a trusted and secure authentication process, where the identity and integrity of vehicles can be verified in a reliable manner. Furthermore, the synchronized view provided by digital twins enables real-time monitoring and anomaly detection, facilitating initiative-taking defence mechanisms against malicious activities.

The outcomes of this research will have significant implications for the field of vehicular networking and cyber-security. The proposed robust authentication framework using digital twin technology has the potential to enhance the security posture of vehicular networks, ensuring the trustworthiness and reliability of communication among vehicles. This, in turn, will enable the deployment of advanced vehicular applications, such as cooperative driving, intelligent transportation systems and autonomous vehicles, with increased confidence and safety. To make the overall driving experience smooth and accidents free, vehicular communication is the most suitable solution. However, for vehicular communication to happen, the vehicles need to exchange a lot of data and information. The user's data is private and should be kept confidential. To address the arising need of securing the data of the users in communication, digital twin technology is combined with vehicular communication. The main motivation behind this paper is to provide an apt authorization model which will ensure security and integrity in communication.

1.4. Contribution

This research paper makes several significant contributions to the field of vehicular networking and cyber-security by proposing a robust authentication framework that leverages digital twin technology. The contributions of this study can be summarized as follows:

- A description of the digital twin technology.
- How digital twin technology can address the difficulties related to communication.
- Computing architecture for autonomous vehicles that is secure for vehicular digital twin communication. In this plan, iTwins converse with one another in the interim to share knowledge.

- To provide communication security and privacy protection, we put forward authentication techniques for vehicular communication.
- Show that the authentication technique has a lower computational cost and satisfies the fundamental security requirements.
- By leveraging digital twin technology, the proposed framework offers enhanced security and privacy features, protecting against attacks such as impersonation, message tampering and replay attacks.
- This contribution paves the way for the realization of advanced vehicular applications that rely on secure and reliable communication among vehicles.
- By considering the practical aspects, the paper provides valuable insights into the real-world applicability and feasibility of the proposed framework.

In summary, this research paper contributes a novel authentication framework for vehicular networking using digital twin technology. By addressing the limitations of traditional authentication mechanisms, enhancing security and privacy, adapting to dynamic network conditions, and enabling advanced vehicular applications, this study significantly advances the field of vehicular networking and cyber-security. The proposed framework holds promise for improving the trustworthiness, reliability, and resilience of vehicular communication, paving the way for safer and more efficient transportation systems.

2. Background of ECC and DY model

ECC (Elliptic Curve Cryptography) is a cryptographic algorithm that plays a significant role in securing Vehicular communication. In this context, ECC offers several advantages and is widely adopted for implementing secure and efficient cryptographic operations [25].

Assume F_z is a prime finite field with a prime number z. An elliptic curve equation over F_z can be defined as $y^2 = x^3 + rx + s \bmod z$, where r and s belong to F_z. The elliptic curve is considered non-singular if the expression $4r^3 + 27s^2 \bmod z$ is not equal to zero. The additive elliptic curve group, denoted as P, consists of points (x, y) where x and y belong to F_z such that $\mathrm{P} = \{(x, y): \mathrm{x}, \mathrm{y} \in F_z; (x, y) \in \xi\} \cup \{\varphi\}, \{\varphi\}$ is the identity element of P.

The group P follows the following operations:

1. For any point $M = (x, y)$ in P, the negation of M is defined as $-M = (x, -y)$ and $P + (-P)$ equals φ.
2. If $M = (x_1, y_1)$ and $N = (x_2, y_2)$ are points in P, their addition $M + N$ is defined as (x_3, y_3), where $x_3 = \alpha^2 - x_1 - x_2 \bmod z$, $y_3 = \alpha(x_1 - x_2) - y_1 \bmod z$ and $\alpha = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \ mod\ z, \ if\ M \neq N \\ \frac{3x_1^2 + a}{2y_1} \ mod\ z, \ if\ M = N \end{cases}$
3. $\mathrm{M} = (\mathrm{x}, \mathrm{y}) \in \mathrm{P}$, scalar multiplication of a point P is defined as $n.M = M + M + M \ldots . + M(n - times)$
4. If p is the base point of P and has an order of n, then $n.p$ equals φ.

The table 2 gives a comparative view of key size between ECC and RSA [26].

Table 2: ECC vs RSA comparison of key size

Item No.	Key size in ECC (in bits)	Key size in RSA (in bits)	Ratio of ECC and RSA
1	163	1024	1:6
2	256	3072	1:12
3	384	7680	1:20
4	512	15360	1:30

ECC offers strong security, efficiency, scalability, and compatibility with existing standards, making it a preferred choice for securing communication. Its ability to provide robust cryptographic operations with smaller key sizes makes ECC well-suited for resource-constrained vehicular environments. By leveraging ECC, communication systems can ensure secure and trusted data exchange, enabling safer and more reliable interactions among vehicles, enhancing road safety and efficiency.

2.1. DY (Dolev-Yao) threat model

The following conditions for the DY model:

- There is an adversary α which has certain capabilities.
- α has the ability to utilize the public communication channel, allowing them to access, manipulate, replay, put some new messages and remove any communication data.
- It is assumed that α is safeguarded and lacks the means to obtain the secret key possessed by other participants.
- α possesses knowledge of the public identities of all users and the server involved.
- α could either be an intruder or an insincere user/server within the underlying system.

3. The proposed protocol

3.1. Network model

Central Authority (CA): For each AV and iTwin, the Central Authority (CA) oversees creating a set of pseudonyms and matching secret points. After iTwin and AV have successfully authenticated one another, the CA creates a group certificate for iTwin so that it can connect with other iTwins. Additionally, CA can track legitimate signatures produced by twins and identify them if they send erroneous messages.

Autonomous Vehicle (AV): AV oversees communicating with their own iTwins and transmitting the data they gathered through fitted sensors to improve service quality.

iTwin: To improve the passenger experience, iTwin oversees processing the data gathered by the corresponding physical lord and offering computation services.

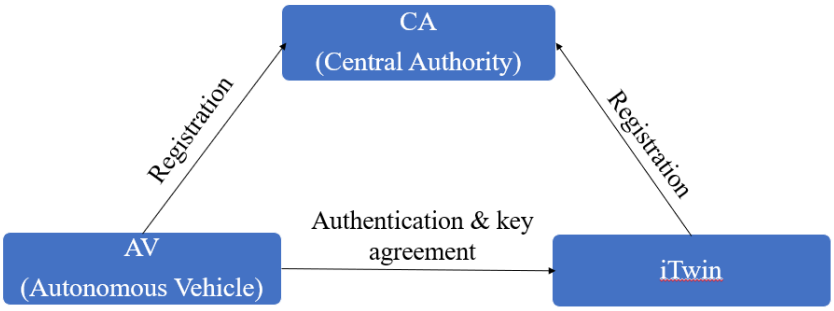

Fig. 3: Registration and authentication model

3.2. Initialization phase

Step 1. CA plays the role of PKG or the third party. CA chooses non-singular EC as $E_q(a,b): y^2 = (x^3 + ax + b) \bmod q$. Select g be the generator of G. Choose random value $c \in Z_q^*$ which is secret key for CA and set public key $PKC = cg$. Choose secure hash function.

Step 2. AV chooses random value $a \in Z_q^*$ set as private key and set public key $PKA = ag$.

Step 3. iTwin chooses random number $t \in Z_q^*$ set as a private key and set public key $PKiT = tg$.

3.3. Registration phase

Step 1. The autonomous vehicle AV inputs its unique identity ID_A and password PW_A. After inputting the login credentials, AV compute $WR_1 = h(ID_A|PW_A)$. It further sends $\{ID_A, PW_A, WR_1\}$ to the central authority in the communication network over a secure channel.

Step 2. The central authority CA generates $C_T \in Z_q^*$ which is a secret key. CA sends the login credentials ID_A and password of the AV, calculated value WR_1 and the newly generated secret key $\{ID_A, PW_A, WR_1, C_T\}$ over the secure channel to the iTwin.

Step 3. The iTwin inputs its ID_T and computes a new value WR_2 which is calculated as $WR_1 \oplus h(ID_T \| ID_A)$. The iTwin further encrypts E_{R1} calculated as $E_{(tg \oplus PW_A)}(WR_2)$. Finally, it sends $\{ER_1, ID_T\}$ over the secure channel back to the central authority.

Step 4. The central authority generates $C_A \in Z_q^*$ and sends $\{E_{R1}, C_A\}$ over the secure channel back to the autonomous vehicle.

Step 5. The autonomous vehicle now again computes $WR_2 = D_{(PKT \oplus PW_A)}(ER_1, ID_T)$. The AV further computes WR_3 calculated as $WR_2 \oplus h(ID_T \| ID_A)$. The AV stores WR_3 in database.

Table 3: Registration phase

AV	CA	iTwin
Input ID_A, PW_A Computes $WR_1 = h(ID_A \| PW_A)$ Sends $\{ID_A, PW_A, WR_1\}$ .....⟹		
	Generates $C_T \in Z_q^*$ Sends $\{ID_A, PW_A, WR_1, C_T\}$ .....→	
		Input ID_T Computes $WR_2 = WR_1 \oplus h(ID_T \| ID_A)$ Encrypts $E_{R1} = E_{(tg \oplus PW_A)}(WR_2)$ Sends $\{ER_1, ID_T\}$ ←.....
	Generates $C_A \in Z_q^*$ Sends $\{E_{R1}, C_A\}$ ←.....	
$WR_2 = D_{(PKT \oplus PW_A)}(ER_1, ID_T)$ Computes $WR_3 = WR_2 \oplus h(ID_T \| ID_A)$ store WR_3 in database.		

3.4. Login and authentication phase

Step 1. The autonomous vehicle AV inputs ID_A^*, PW_A^* and further computes W^* calculated as $h(ID_A^* \| PW_A^*)$. To authenticate the communication, it verifies whether W^* is equal to WR_3^*. If W^* is equal to WR_3^*, it generates $a \in Z_q^*$ and computes W_1which is calculated as $h(C_A \| ID_A \| ID_T)$. It further finds the value of K_1 calculated as $h(PW_A \| ID_A \| ID_T)$. AV encrypts E_1 as $E_{K_1}(ag, W_1, C_A)$ and sends $M_1 = \{E_1, T_1\}$ via open channel in the communication network.

Step 2. On receiving the inputs in the open channel, the iTwin verifies whether $T_2 - T_1 \leq \triangle T$. It further computes K_1^* calculated as h$(PW_A \| ID_A \| ID_T)$. The iTwin decrypts $(ag, W_1, C_A) = D_{K_1^*}(E_1)$ and computes $W_1^* = h(C_A \| ID_A \| ID_T)$. The iTwin verifies whether W_1^* is equal to W_1. If W_1^* is equal to W_1, it generates $b \in Z_q^*$. The iTwin does computations for SK_T, W_2 and K_2 which are calculated as $h(T_3 \| bag \| ID_T \| C_A \| ID_A)$, $h(ag \| bg \| T_3 \| C_A \| C_T)$ and $h(C_A \| tg \| ID_T)$ respectively. It further encrypts E_2 as $E_{K_2}(W_2, bg, T_3)$ and sends $M_2 = \{E_2, T_3\}$ via open channel.

Table 4: Login and authentication phase

AV	iTwin
Inputs ID_A^*, PW_A^*	
Computes $W^* = h(ID_A^* \parallel PW_A^*)$	
Verifies $W^* \stackrel{?}{=} WR_3^*$	
Generates $a \in Z_q^*$	
Computes $W_1 = h(C_A \parallel ID_A \parallel ID_T)$	
Computes $K_1 = h(PW_A \parallel ID_A \parallel ID_T)$	
Encrypts $E_1 = E_{K_1}(ag, W_1, C_A)$	
Sends $M_1 = \{E_1, T_1\}$	
……⟹	
	Verifies $T_2 - T_1 \leq \triangle T$
	Computes $K_1^* = \mathrm{h}(PW_A \parallel ID_A \parallel ID_T)$
	Decrypts $(ag, W_1, C_A) = D_{K_1^*}(E_1)$
	Computes $W_1^* = h(C_A \parallel ID_A \parallel ID_T)$
	Verifies $W_1^* \stackrel{?}{=} W_1$ if yes
	Generates $b \in Z_q^*$
	Computes $SK_T = h(T_3 \parallel bag \parallel ID_T \parallel C_A \parallel ID_A)$
	Computes $W_2 = h(ag \parallel bg \parallel T_3 \parallel C_A \parallel C_T)$
	Computes $K_2 = h(C_A \parallel tg \parallel ID_T)$
	Encrypts $E_2 = E_{K_2}(W_2, bg, T_3)$
	Sends $M_2 = \{E_2, T_3\}$
	⟸……
Verifies $T_3 - T_2 \leq \triangle T$	
Computes $K_2^* = h(C_A \parallel PKT \parallel ID_T)$	
Decrypts $(W_2, bgT_3) = D_{K_2^*}(E_2)$	
Computes $W_2^* = h(ag \parallel bg \parallel T_3 \parallel C_A \parallel C_T)$	
Verifies $W_2^* \stackrel{?}{=} W_2$ if yes	
Computes $SK_A = h(T_3 \parallel abg \parallel ID_T \parallel C_A \parallel ID_A)$	
Hence, $SK = SK_A = SK_T$	

Step 3. On receiving the inputs back in the open channel, the autonomous vehicle verifies whether $T_3 - T_2 \leq \triangle T$. The AV computes K_2^* as $h(C_A \parallel PKT \parallel ID_T)$ and decrypts $(W_2, bgT_3) = D_{K_2^*}(E_2)$. It further computes W_2^* as $h(ag \parallel bg \parallel T_3 \parallel C_A \parallel C_T)$. Later, it verifies whether W_2^* is equal to W_2. If W_2^* is equal to W_2, it computes session key SK_A as $h(T_3 \parallel abg \parallel ID_T \parallel C_A \parallel ID_A)$. Hence, $SK = SK_A = SK_T$ which ensures authentication and communication can happen securely.

4. Security analysis

In this section, we are performing the security analysis of the proposed model for authentication as below:

4.1. Formal security analysis:

Formal security analysis involves proof through theorems.

Theorem: $P_Z^{\mathrm{CurrModel}} \leq \frac{ah^2}{2^l} + \frac{a_s}{2^{l-1}} + \frac{(as+ae)^2}{2^{l+1}} + 2\mathrm{ah}\left(P_Z^{ECDHModel}(a)\right) + 2\frac{a_s}{M} + 2\frac{a_s}{N}$

Here, $P_Z^{\mathrm{CurrModel}}$ denotes the chance of success for probabilistic polynomial time bounded. γ denotes the semantic security of the proposed model. $P_Z^{ECDHModel}$ is the chance of success z of solving the elliptic curve computational

Diffie-Hellman problem. l denotes the length of bits in the digest. M is the dictionary of the password. N denotes the dictionary of the identity. z looks for a_s times "Send," a_e times "Execute" and a_h times "H" to breach the security of the proposed model.

Proof: This is proved through a number of rounds where z can attack the proposed model in Round_0 and z has no safety in Round_5. Round_i and Round_{i+1} are almost same until E event happens. Here event ξ implies that the value of i will range between 0 to 5. Hence, $|Prob[\xi_{i+1}] - Prob[\xi_i]| \leq Prob[E]$

- Round_0: In this round, z can find out the bits. So,
$$P_z^{CurrModel} = |2Prob[\xi_0] - 1| \quad (1)$$
- Round_1: This round is similar to the previous one. But here, z calculates the hash value and performs execution, revelation, sending, corruption and testing to attack the model. So,
$$Prob[\xi_1] = Prob[\xi_0] \quad (2)$$
- Round_2: In this round, the chance of colliding of the hash can go up to $\frac{ah^2}{2a}$. Similarly, the chance of colliding in the simulation is maximum at $\frac{(a_s+a_e)^2}{2^{l+1}}$. So,
$$Prob[\xi_2] - Prob[\xi_1] \leq \frac{ah^2}{2a} + \frac{(a_s+a_e)^2}{2^{l+1}} \quad (3)$$
- Round_3: In this round, z finds out the attributes for authentication. This round will be different from the last round if the user or the server denies the authentication. So,
$$Prob[\xi_3] - Prob[\xi_2] \leq \frac{a_s}{2^J} \quad (4)$$
- Round_4: In this round, z calculates ECDH attributes. So,
$$Prob[\xi_4] - Prob[\xi_3] \leq ah\left(P_z^{ECDHModel}(a)\right) \quad (5)$$
- Round_5: In this round, z can get the session keys with a maximum chance of $\frac{ah^2}{2^l}$. So,
$$Prob[\xi_5] - Prob[\xi_4] \leq \frac{ah^2}{2a} \quad (6)$$

Here, $Prob[\xi_5] = \frac{1}{2}$. Also, the chances of z performing offline password guessing attack and identity guessing attack are $\frac{a_s}{M}$ and as $\frac{a_s}{N}$ respectively. Using the outputs of Round_0 and Round_5, $P_Z^{\text{CurrModel}} \leq \frac{ah^2}{2^l} + \frac{a_s}{2^{l-1}} + \frac{(a_s+a_e)^2}{2^{l+1}} + 2ah\left(P_z^{ECDHModel}(a)\right) + \frac{2a_s}{M} + \frac{2a_s}{N}$

4.2. Informal security analysis:

Informal security analysis is done by checking the model against various security attributes and multiple types of external attacks.

- **Off-line password guessing attack**: Suppose the attacker guesses the user ID ID_P and password PW_P. The random value $b \in Z_q$ is generated and performs $PWQ = h(PW_P \parallel ID_P \parallel b)$. The number of values for the ID and password are limited but it is almost impossible to guess the value of b.
- **Anonymity:** During authentication, both AVs and their individual iTwins choose unused pseudonyms created by CA to authenticate one another. Only CA may deduce the identity of the participants from the pseudonyms. The server uses ID_A for the user and ID_S for the server and hence real identities are hidden.
- **Replay attack:** In the authentication stage, it verifies $W_2^* \stackrel{?}{=} W_2$. If the attacker tries to perform the replay attack, $SK_A = h(T_3 \parallel abg \parallel ID_T \parallel C_A \parallel ID_A)$. It will try $SK = SK_A = SK_T$ which is not possible. The proposed model takes into consideration the time stamps at all steps and hence is safe against the replay attack.
- **User impersonation attack:** The attacker may try to impersonate by using ID ID_P and password PW_P. As explained under offline password guessing attack and smart card loss attack, even if the attacker tries to impersonate the genuine user either by stealing passwords or any other method, the proposed model is secure.

- **Server spoofing attack**: Even if the attacker tries to spoof the server, he will not be able to calculate the value of $SK_A = h(ID_T \parallel ID_A \parallel C_A \parallel C_T \parallel xyg \parallel T_3)$and hence the model is secure.
- **De-synchronization attack:** This model does not require either the user with ID_A or the server with ID_S to undergo synchronization, making the model secure against this attack.
- **Insider attack:** In the proposed model, the user sends $\{ID_A, PW_A, HR_1, C_T\}$ where C_T is a random value. Any internal user would not be able to get the PW_A. Hence, this model is safe against insider attacks.
- **Unlinkability:** In authentication, malicious AVs and iTwins choose an unused pseudonym to authenticate each other, preventing them from linking based on that pseudonym's constant use.

5. Performance analysis

In this section, we do a comparison with other models and frameworks in terms of security and functionality, computation cost and communication cost. The performance analysis is particularly important as it gives more clarity on how secure the proposed model is and how it appears when compared to other past models. In this section, we will compare the proposed framework with related frameworks like Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31].

5.1. Security and functionality

Table 5 shows the security and functionality attributes of the proposed framework with other frameworks like Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31]. The last column shows a total of the requirements which are satisfied by the given framework.

In the figure 4, the performance analysis in terms of security and functionality clearly shows that the proposed model satisfies all the ten requirements. Some of the frameworks satisfy only 2 or 4 or 6 requirements as against the proposed framework.

Table 5: Comparison of features of security and functionality

Frameworks/Attributes	*OPGA*	*AN*	*RA*	*UIA*	*SA*	*DSA*	*IA*	*UN*	*FA*	*UT*	*Total*
Noori et al. [27]	×	√	√	×	×	×	×	×	×	×	2
Yang Wu et al. [28]	√	√	×	√	×	×	√	×	×	×	4
Chen et al. [29]	√	×	√	×	×	×	×	×	×	×	2
Zhang et al. [30]	√	×	√	√	×	×	√	×	×	×	4
Fan Wu et al. [31]	√	√	×	×	×	√	√	×	√	√	6
Proposed	√	√	√	√	√	√	√	√	√	√	10

Here OPGA: Offline password guessing attack, AN: Anonymity, RA: Replay attack, UIA: User Impersonation attack, SA: Spoofing attack, DSA: Desynchronization attack, IA: Insider attack, UN: Unlinkability, FA: Forgery Attack, UT: User Traceability

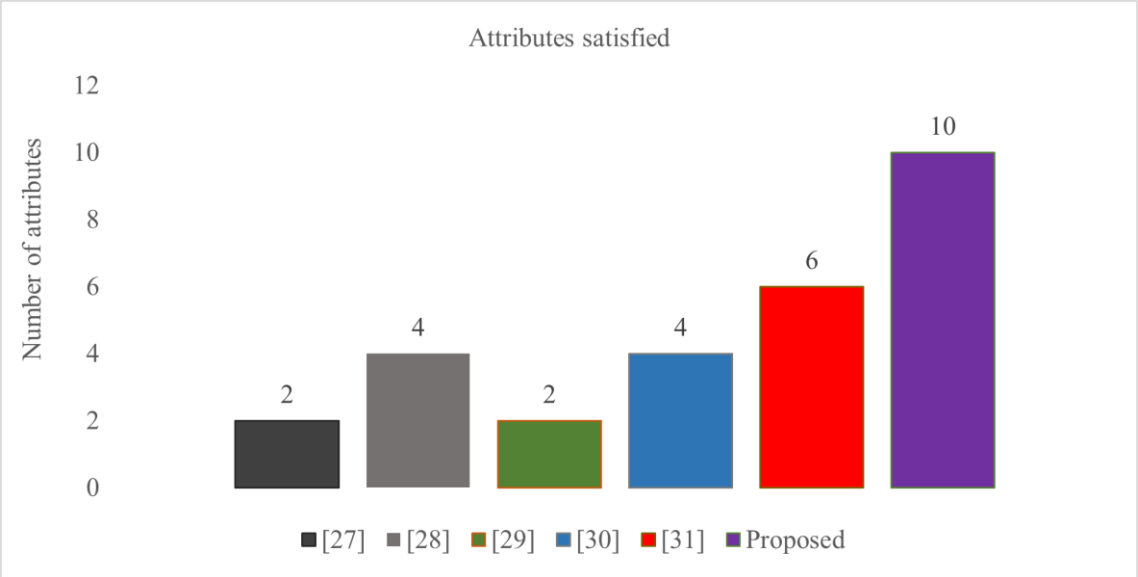

Fig. 4: Security and functionality

5.2. Computation cost

This section compares the computation cost of the proposed framework to other frameworks like Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31]. The computation cost has been derived as the results from the study conducted in paper [32]. In Table 6, we have specified the time taken in completing various operations.

Table 6: Computation timing for operations

Operations	Notation	Time in ms (approx.)
Elliptic curve point multiplication computation time	T_{PM}	0.064
Time to execute a fuzzy extraction function	T_F	0.05665
Time to perform a hash operation	T_H	0.003204
Running times of symmetric encryption	T_S	0.0211525
Running times of symmetric decryption	T_D	0.0211525
Scalar multiplication in elliptic curve cryptosystem	T_{BKG}	0.294437

Table 7 calculates the computation cost for the proposed framework to be $11T_H + 4T_{S/D}$ and provides comparison with the other frameworks proposed by Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31]. In the figure 5, it can be clearly seen that the computation cost for the proposed framework is lesser than all the other frameworks.

Table 7: Comparison of computation cost

Frameworks	Computation cost	Time in ms (approx.)
Noori et al. [27]	$2T_{PM} + T_H + 8T_{BKG}$	0.3968
Yang Wu et al. [28]	$T_F + 31T_H$	0.156
Chen et al. [29]	$2T_S + 23T_H + T_D$	0.1371
Zhang et al. [30]	$T_F + 28T_H$	0.1464
Fan Wu et al. [31]	$T_{BKG} + 32T_H$	0.397
Proposed	$11T_H + 4T_{S/D}$	0.1199

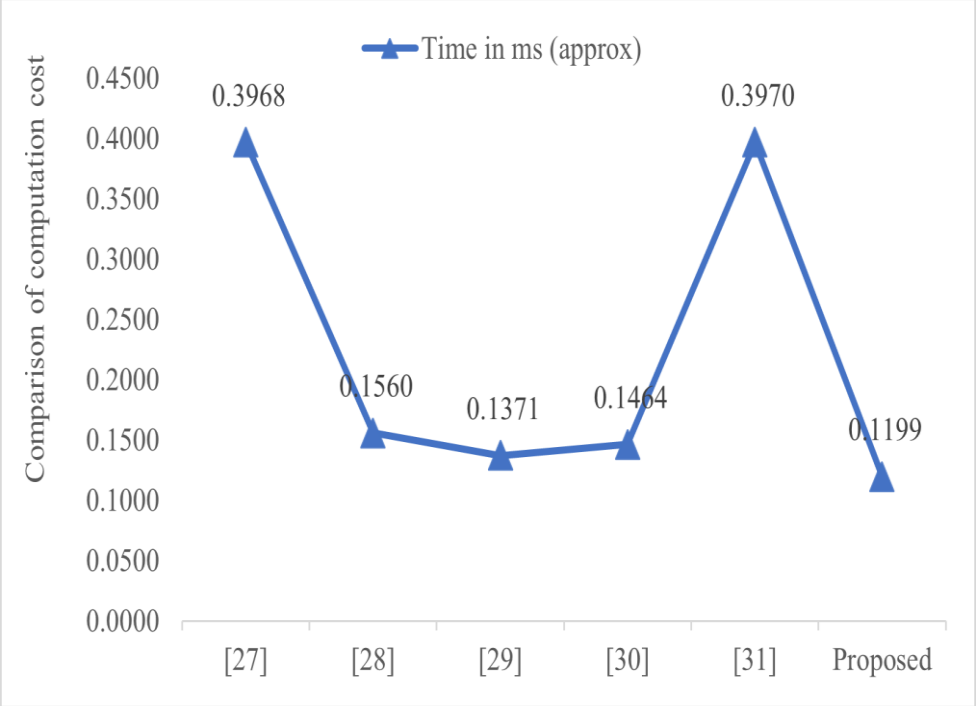

Fig. 5: Comparison of computation cost

5.3. Communication cost

The Table 8 calculates the communication cost for the proposed framework compared to other frameworks like Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31]. The communication cost of encryption, time stamp, hash, string and identity are 256 bits, 32 bits, 256 bits, 160 bits and 160 bits respectively. In the proposed model, the first message is $M_1 = \{E_1, T_1\}$ and the second message is $M_2 = \{E_2, T_3\}$. These two messages include two encryptions and two timestamps. Thus, the communication cost for the proposed model is 256 + 32 + 256 + 32 = 576 bits. The communication cost for the proposed framework is lower than that of Noori et al. [27], Yang Wu et al. [28], Chen et al. [29], Zhang et al. [30] and Fan Wu et al. [31]. In figure 6, it can be clearly seen that the communication cost of the proposed framework is the least among all the peer frameworks.

Table 8: Comparison of communication cost

Frameworks	Communication cost in bits
Noori et al. [27]	960
Yang Wu et al. [28]	2944
Chen et al. [29]	6400
Zhang et al. [30]	4544
Fan Wu et al. [31]	3712
Proposed	576

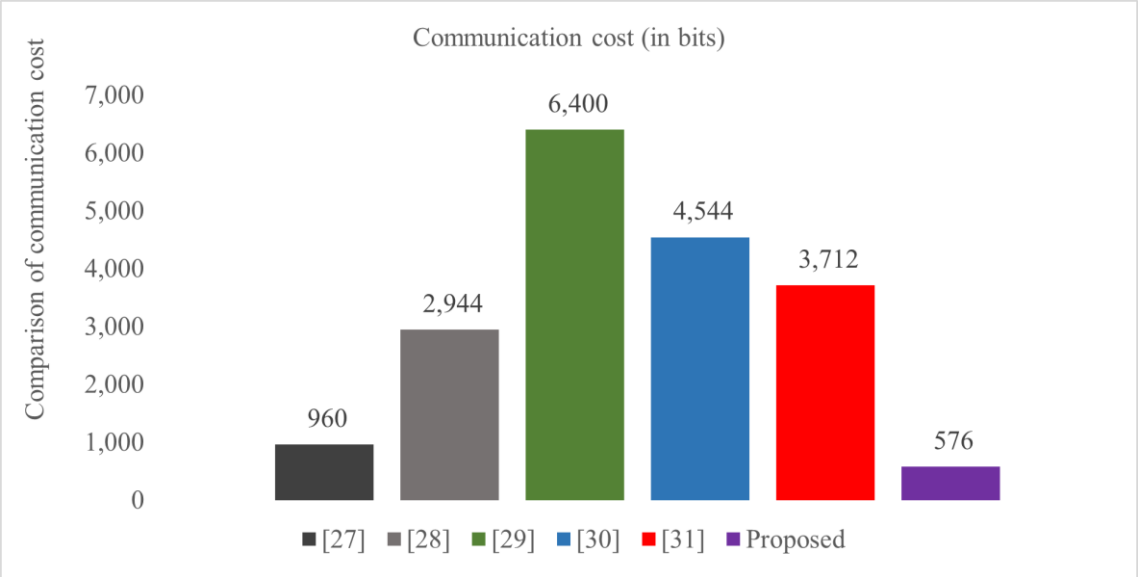

Fig. 6: Comparison of communication cost

6. Future directions and conclusion

In conclusion, this research paper has presented a robust authentication framework for vehicular networking using digital twin technology. The framework addresses the unique challenges and requirements of vehicular networks, offering an innovative approach to enhance authentication, security, and privacy in communication. The proposed authentication framework leverages the power of digital twin technology to create virtual replicas of vehicles, capturing their characteristics, behaviour, and context. By establishing a synchronized and trusted view of the vehicles, the framework enables reliable authentication mechanisms that prevent unauthorized access, mitigate impersonation attacks, and protect against message tampering and replay attacks. The integration of digital twin technology offers real-time monitoring, anomaly detection and proactive defence mechanisms, ensuring the integrity and confidentiality of exchanged information in vehicular networks.

The existing vehicular communication systems can only issue driver warnings. The next generation of systems will be built with autonomous driving in mind because the technology is well beyond the infancy stage. In order to avert disaster, the system will be able to take control of a vehicle when it detects impending danger. The communication systems have the potential to significantly increase traffic productivity since they can improve driving safety and efficiency. They could have a significant impact on small towns and major cities all over the world. They might also be helpful in reducing traffic congestion, which directly lowers carbon emissions in urban areas. The major concern is security. To maintain security, we offer specific authentication protocols for vehicular communication. The security analysis and performance assessment demonstrate that our suggested protocol meet the essential security standards while having a lower cost of computing.

References

[1] Palla, K.: The Rise Of Digital Twin Technology. Forbes. https://www.forbes. com/sites/forbestechcouncil/2022/08/03/the-rise-of-digital-twin-technology/ ?sh=47ff70302f97
[2] Marr, B.: What Is Digital Twin Technology - And Why Is It So Important? Forbes. https://www.forbes.com/sites/bernardmarr/2017/03/06/ what-is-digital-twin-technology-and-why-is-it-so-important/?sh=60b487f22e2a
[3] IBM: What is a digital twin?? https://www.ibm.com/topics/ what-is-a-digital-twin
[4] PTC: Digital Twin: Transforming How We Make Sense of Data. https://www. ptc.com/en/industry-insights/digital-twin

[5] TWI: What is digital twin technology and how does it work? https://www. twi-global.com/technical-knowledge/faqs/what-is-digital-twin
[6] Shaw, K., Fruhlinger, J.: What is a digital twin and why it's important to IoT. Networkworld. https://www.networkworld.com/article/3280225/ what-is-digital-twin-technology-and-why-it-matters.html
[7] Kumar, V.: Rsfvc: Robust biometric-based secure framework for vehicular cloud networking. IEEE Transactions on Intelligent Transportation Systems, 1–11 (2023) https://doi.org/10.1109/TITS.2023.3322960
[8] Horng, G., Yang, C.S.: Key authentication scheme for cryptosystems based on discrete logarithms. Computer Communications 19(9-10), 848–850 (1996) https: //doi.org/10.1016/S0140-3664(96)01112-7
[9] Chien, H., Jan, J.-K., Tseng, Y.-M.: An efficient and practical solution to remote authentication: Smart card. Computers Security 21 (2002) https://doi.org/10. 1016/S0167-4048(02)00415-7
[10] Nam, J., Kim, M., Paik, J., University, P., Lee, Y.: A provably-secure ecc-based authentication scheme for wireless sensor networks. Sensors 14 (2014) https:// doi.org/10.3390/s141121023
[11] Rase, S., Dharavath, S.: Review of mobile cloud computing framework and authentication problems. International Journal of Scientific Engineering Research 5(2) (2014). https://www.ijser.org/paper/ Review-of-Mobile-Cloud-Computing-Framework-and-Authentication-Problems. Html
[12] Ling, C.-H., Lee, C.-C., Yang, C.-C., Hwang, M.-S.: A secure and efficient onetime password authentication scheme for wsn. International Journal of Network 16 Security 19(2), 177–181 (2015) https://doi.org/10.6633/IJNS.201703.19(2).02
[13] Surekha, B., Narayana, K.L., Jayaprakash, P., Vorugunti, C.: A realistic lightweight authentication protocol for securing cloud based rfid system. IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (2016) https://doi.org/10.1109/CCEM.2016.018
[14] Tewari, A., Gupta, B.B.: A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices. International Journal of Advanced Intelligence Paradigms 9 (2017) https://doi.org/10.1504/IJAIP.2017.082962
[15] Gupta, B.B., Quamara, M.: An identity based access control and mutual authentication framework for distributed cloud computing services in iot environment using smart cards. Procedia Computer Science 132, 189–197 (2018) https://doi. org/10.1016/j.procs.2018.05.185
[16] Vel´asquez, I., Caro, A., Rodr´ıguez, A.: Multifactor authentication methods: A framework for their comparison and selection. Computer and Network Security (2019) https://doi.org/10.5772/intechopen.89876
[17] Eldow, A., Shakir, M., Talab, M.A., Muttar, A.K.: Literature review of authentication layer for public cloud computing: a meta-analysis. ARPN Journal of Engineering and Applied Sciences 14(10) (2019). https://www.academia.edu/ 39797246/LITERATURE REVIEW OF AUTHENTICATION LAYER FOR PUBLIC CLOUD COMPUTING A META ANALYSIS
[18] ALnwihel, L.K., Khan, A.R.: A novel cloud authentication framework. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 1302–1308 (2020) https://doi.org/10.1109/CSCI51800.2020.00243
[19] Al-Refai, H., Batiha, K., Al-Refai, A.M.: An enhanced user authentication framework in cloud computing. International Journal of Network Security Its Applications 12(2), 59–75 (2020) https://doi.org/10.5121/ijnsa.2020.12204
[20] Al-Refai, H., Batiha, K., Al-Refai, A.M.: A robust user authentication framework for bigdata. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 1256–1261 (2021) https:// doi.org/10.1109/ICICV50876.2021.9388505
[21] Mohammad, A., Al-Refai, H., Alawneh, A.A.: User authentication and authorization framework in iot protocols. Computers 11(10), 147 (2022) https://doi.org/ 10.3390/computers11100147
[22] Raj, A.S.A., Venkatesan, R., Malathi, S., Kumar, V.D.A., Thenmozhi, E., Dhandapani, A., Kumar, M.A., Chitra, B.: A mathematical queuing model analysis using secure data authentication framework for modern healthcare applications. Journal of Sensors (2022) https://doi.org/10.1155/2022/8397635 17
[23] Khan, A.R., Alnwihel, L.K.: A brief review on cloud computing authentication frameworks. Engineering, Technology and Applied Science Research 13(1), 9997– 10004 (2023) https://doi.org/10.48084/etasr.5479

[24] Wang, R., Liu, X., Liu, D., Zhang, H., Ma, L., Wang, Y., Liu, H., Chen, J., Li, Z.: An sm9-based secondary authentication framework for 5g technology. Journal of Circuits, Systems and Computers 32(6) (2023) https://doi.org/10.1142/ S0218126623500949

[25] Verma, S.K., Ojha, D.B.: A discussion on elliptic curve cryptography and its applications. International Journal of Computer Science Issues 9(1) (2012)

[26] Kumar, V., Ahmad, M., Kumari, A., Kumari, S.: Sebap: A secure and efficient biometric-assisted authentication protocol using ecc for vehicular cloud computing. International Journal of Communication Systems 34(4) (2021) https: //doi.org/10.1002/dac.4103

[27] Noori, D., Shaker, H., Torshiz, M.N.: An elliptic curve cryptosystem-based secure rfid mutual authentication for internet of things in healthcare environment. EURASIP Journal on Wireless Communications and Networking (64) (2022) https://doi.org/10.1186/s13638-022-02146-y

[28] Wu, T.-Y., Yang, L., Lee, Z., Chu, S.-C., Kumari, S., Kumar, S.: A provably secure three-factor authentication protocol for wireless sensor networks. Wireless Communications and Mobile Computing (2021) https://doi.org/10.1155/2021/ 5537018

[29] Chen, C.-M., Liu, S., Li, X., Kumari, S., Li, L.: Design and analysis of a provable secure two-factor authentication protocol for internet of things. Security and Communication Networks (2022) https://doi.org/10.1155/2022/4468301

[30] Wu, T.-Y., Meng, Q., Kumari, S., Zhang, P.: Rotating behind security: A lightweight authentication protocol based on iot-enabled cloud computing environments. Sensors 22(10) (2022) https://doi.org/10.3390/s22103858

[31] Wu, F., Li, X., Xu, L., Vijayakumar, P., Kumar, N.: A novel three-factor authentication protocol for wireless sensor networks with iot notion. IEEE Systems Journal 15(1), 1120–1129 (2021) https://doi.org/10.1109/JSYST.2020.2981049

[32] Kumari, A., Jangirala, S., Abbasi, M.Y., c, V.K., Alam, M.: Eseap: Ecc based secure and efficient mutual authentication protocol using smart card. ScienceDirect 51 (2020) https://doi.org/10.1016/j.jisa.2019.102443