International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 13s,2025
https://theaspd.com/index.php

A Secure And Efficient Protocol For Vehicle Digital Twin Networks Using Elliptic Curve Cryptography

Dheeraj Tiger[1], Nishu[2], Vinod Kumar[3,*] and Anshu Malhotra[4]
[1]Department of Applied Sciences, The NorthCap University, Gurugram-122017, India, dheerajtiger@gmail.com
[2]Department of Computer Science and Engineering, The NorthCap University, Gurugram-122017, India, sethinishu@gmail.com
[3]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi 110032, India, vinod.iitkgp13@gmail.com & vkmaths@shyamlal.du.ac.in
[4]School of Engineering and Technology, K. R. Mangalam University Gurugram-122103, India, anshu@krmangalam.edu.in

Abstract: *Autonomous cars (AVs) are revolutionizing transportation today, with digital twins (DTs) contributing significantly to their design and operation. DTs refer to virtual copies that mimic the behaviour of AVs in different environments. Even though there are advantages associated with the integration of AVs and DTs, there are critical privacy and safety issues involved. In response to this, we suggest a safe key agreement protocol based on Elliptic Curve Cryptography (ECC) for communication between AVs and DTs. This work discusses recent security advancements, gives possible attack scenarios, and analyses the computational and communication efficacy of the proposed protocol. Our security analysis is consistent with the fact that the scheme provides secure and efficient communication. Experimental findings testify that the proposed protocol satisfies all requirements for security and is more efficient than previous methods.*
Keywords: *Autonomous vehicles, Digital twins, Vehicle networks, ECC, Security and Privacy*

1. INTRODUCTION

The Digital Twin (DT) has become a revolutionary driving force in frontier technologies, radically transforming the design, monitoring, and optimization of complicated systems [1]. A DT is a digital twin or virtual model of a physical entity—either a system, process, or product. Such a digital twin captures the dynamic characteristics, interactions, and dynamics of its physical equivalent in real-time, thus serving as an important link between the physical and digital realms. It allows for real-time observation, simulation, and decision-making, and hence serves as an effective tool for improving productivity, driving innovation, and enhancing operational performance across various industries. DTs are usually created from data gathered by sensors, cameras, and other monitoring units that constantly monitor the physical object or system [2]. This data enables high-fidelity digital simulation of the physical asset under diverse conditions. Researchers, engineers, and analysts leverage these simulations to enhance the design of products, optimize manufacturing operations, and anticipate the need for maintenance. The use of DTs has now reached a state of ubiquity, crossing various industries such as healthcare, manufacturing, smart cities, architecture, aerospace, and most importantly, intelligent transportation systems. As DTs become increasingly intertwined with systems in the real world, it becomes increasingly critical to provide secure communication, data integrity, and confidentiality, particularly in safety-critical applications like autonomous vehicles (AVs). As the environment of intelligent transportation changes rapidly, the introduction of AVs is a revolutionary technological benchmark [3]. These autonomous cars represent a paradigm change in how transportation is envisioned, deployed, and perceived. In contrast to traditional cars, AVs are integrated with an intricate suite of sensors, cameras, radars, lidars, artificial intelligence (AI) units, and control systems. These all combined enable the car to sense its surroundings, process information, make choices, and move on its own without driver input [4].

Table 1: Features of VDT networks

Properties of Vehicular Digital Twin Networks – Comparison Table

Property	Description	Benefits
Real-Time Synchronization	Live data exchange between physical vehicle and its digital twin.	Immediate awareness of vehicle state; low-latency decision-making.
Bidirectional Data Flow	Data flows both from vehicle to twin and from twin to vehicle.	Enables feedback, control, and remote updates.
High-Fidelity Modeling	Accurate replication of vehicle systems, behavior, and environment.	Improves simulation accuracy and diagnostics.
Context Awareness	Incorporates road, traffic, weather, and environmental data.	Supports proactive route planning and situational decisions.
Predictive Analytics	Uses AI/ML to forecast faults, behaviors, and events.	Enhances safety, efficiency, and reliability.
Scalability & Interoperability	Supports large-scale deployment across multiple platforms.	Suitable for smart cities, fleet systems, and heterogeneous environments.
Edge-Cloud Collaboration	Division of tasks between edge devices (fast response) and cloud (heavy compute).	Reduces latency and network congestion.
Security & Privacy	Ensures encrypted communication and privacy-aware data handling.	Protects against cyber threats and data misuse.
Self-Adaptivity	System adapts to changing conditions in vehicle and network.	Improves resilience and system responsiveness.
Lifespan Integration	Covers the entire lifecycle of the vehicle.	Enables long-term analysis and product improvement.

The design and deployment of AVs are motivated by the larger vision of enhancing road safety, optimizing transportation efficiency, lowering environmental footprints, and boosting accessibility. As the automobile sector continues to pump significant investments in research and development, the dream of fully autonomous mobility is slowly becoming an imminent reality [5]. But as this revolution unfolds, a new range of challenges—mainly security, privacy, and dependability-related—arises. As AVs drive in open and dynamic spaces, they are susceptible to possible cyber-attacks, data leakages, and manipulation of systems. To counter these issues, effective and robust cryptographic techniques are required. Of the various contemporary cryptographic methods, Elliptic Curve Cryptography (ECC) is a hopeful method owing to its security, scalability, and computational lightness. ECC offers good security with much lower key sizes than conventional methods such as RSA or DSA, making it perfectly suitable for resource-limited environments like AVs and DT systems [6]. Considering the dynamic and connected nature of AVs and their respective DTs, ECC is a suitable option for authenticating the communication links between them. It does not only reduce computational and energy costs but also delivers the required cryptographic power for ensuring data integrity, confidentiality, and authenticity. This is especially relevant because the coordinated ecosystem of DTs and AVs is dependent on the sharing of real-time information, sensor inputs, command signals, and status signals. Any breakdown in the security of such data can have grave consequences, including failure of operations and safety risks. This paper stresses the need to establish a strong and lightweight key agreement protocol for AV-DT communication systems. The conventional key

exchange methods are usually susceptible to a range of attacks, including man-in-the-middle, replay, impersonation, and denial-of-service (DoS). These weaknesses, if taken advantage of, can jeopardize the entire AV-DT network. A more evolved and secure method is thus required. Our interest in ECC-based key agreement protocols is due to its ability to confront these weaknesses adequately, particularly in scenarios where there are constrained computational resources, storage, and bandwidth [7]. ECC's appropriateness for lightweight cryptographic computations makes it a prime candidate for AVs and DTs, which tend to run with stringent performance and power limits. This work also examines some of the different security threats and analyses the computational and communication cost of current cryptographic protocols. We introduce a new ECC-based key agreement protocol particularly designed to address key issues such as latency, scalability, and energy efficiency. The proposed protocol provides secure communication by establishing a shared mutually authenticated session key between AVs and their DTs, thus preventing typical attacks and facilitating trust within the communication process [8].

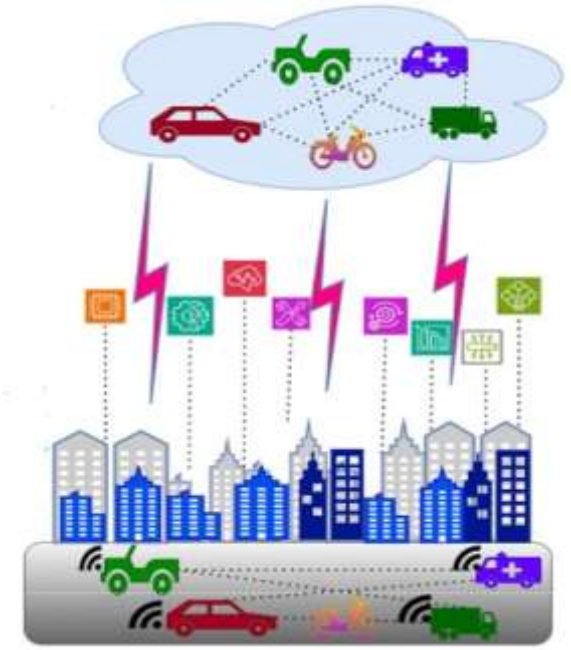

Figure 1: AV and Twin networks

1.1 Motivation and contribution

Modern transportation needs to be secure and trustworthy while this requires secure data transfer between an autonomous vehicle, and its virtual replica; the security efficacy and magnitude of conventional techniques of keys agreement are typically compromised owing to their aptness for heavy data exchange communication demands in AV's. Another solution is also present in an elliptic curve cryptography solution with improved and strong computing for small key size regarding privacy and security issues have been suggested. Entities need to authenticate each other prior to sharing sensitive information. In the last couple of years, many ECC-based protocols for authentication and key agreement have been suggested; however, they all become redundant. In an effort to propose an appropriate key agreement for AVs and DTs based on ECC, we have introduced a framework. The following are the characteristics of the proposed framework:

- We give an ECC-based key agreement approach that well performs for AVs and DTs. The session key is generated with the help of a central authority.
- There has been a detailed discussion regarding the informal security features.
- Comparison of communication and computation costs of the suggested protocol with various schemes.

1.2 Organization of the paper

Section 2 is the related work. Section 3 is the mathematical concepts and notations. Section 4 is the proposed protocol. Section 5, the security analysis of the proposed protocol. Section 6 is performance analysis. Section 7 provides the conclusion.

2. RELATED WORKS

A survey paper was suggested in 2019 by Kuutti et al. [9]. In their paper, they provided a survey of deep learning-based techniques for AV control. The method was categorized into three forms: simultaneous lateral and longitudinal control strategies, longitudinal and lateral, respectively, and specifically acceleration and braking, steering. Meanwhile, there are some obvious overlaps between Perception and vehicle control solutions, emphasis in this work has been on the former. Evidence was provided that there has been a substantial upsurge in research interest in this area recently and that this is likely to continue. A study on DT-based AV maintenance needs was suggested by Khan et al. [10] in 2020. This paper used the idea of the DT and new developments in machine learning to investigate autonomous maintenance. The data that was found presented key needs and how they could potentially be satisfied. Generative learning is becoming increasingly popular in applications within engineering and is a very potentially enabling idea. Several (computer) models have also been employed by practitioners for monitoring and troubleshooting at the system level. Sadly, the accuracy (and interpretation) of models are compromised due to the quality of the data being used in the process and many of the potential users seem not to have the information needed to find or use the right data. A research on the development of AVs was proposed by Alghodhaifi et al. [11] in 2021. The poll has surveyed all these aforementioned technologies to identify how optimally they are utilized by vehicle-to-user (V2X) communication applications. The key features of the technology used for short-range communication are explained, as well as how it can be applied for certain V2X applications such as vehicle identification, forward collision warning, and toll check that have no need for high latency. They cannot, however, govern applications like remote driving and maintenance. Due to its low rates of data and latency, it is able to provide the maximum level of information collectively and offers shortest latency among the four short-range technologies. Parekh et al. [3] have published a renewed review on AVs in 2022. The paper spoke about, highlighted, and criticized technological trends regarding autonomous driving based on this survey. This research also examined recent development in autonomous driving along with case studies. Security, There are many of the nontechnical challenges, such as privacy, path planning, and safety issues related to this research, that are numerous issues. Consumer trust, governance, and public attitudes towards autonomous driving are just a few examples of nontechnical challenges that are crucial to the extensive use of AVs and related technology. One paper was recently put forward by Hossein et al. [12]. The This research encompasses the history, development, and numerous stages of DT technology application. This research emphasizes the new DT technologies for smart electric vehicle applications. Such technologies are autonomous motion control, cars as a service, driver aid systems, predictive mobility, vehicle-to-cloud-based driver assistance systems, and the controversy regarding the Petri net model.

3. PRELIMINARIES

We describe here the necessary mathematical methods and terminology to properly investigate and comment on the proposed framework.

3.1 Notation

Table 1 lists the key notation utilized in the suggested framework.

Table 2: Symbol and meaning

Symbol	Meaning
EC	Elliptic curve
ECC	Elliptic curve cryptography
A	Attacker
G	EC based additive group
q	The large prime number
$Twin_i$	i^{th} $Twin$ vehicular cloud
$\|\|$	Concatenation operation
$\oplus$	XOR operation
SK	Session Key
$E_q\ (a, b)$	Elliptic curve over finite prime field F_q

AV	Autonomous vehicles
$h(.)$	Hash function
g	The base point of the G
PW_A	Password of AV
ID_A	Identity of AV

3.2 Elliptic curve cryptography

Let q be a prime of large and $a, b \in Z_q^*$, where Z_q^* is a finite field. Assuming $4a^3 + 27b^2 \neq 0 \pmod q$, we have the equation for a non-singular elliptic curve $E_q(a,b)$ defined over Z_q^*: $E_q(a,b) : y^2 \equiv x^3 + ax + b \ (mod\ q)$. The additive group G associated to the elliptic curve is given by $G = \{(x,y): x, y \in Z_q^*, (x,y) \in E_q\} \cup \{\Theta\}$. Because the identity element (zero element) of Θ is called asymptotic point or identity element for G. The operations of the group G are as follows [13, 14]:

- **Scalar Multiplication:** Let $P \in E_q(a,b)$. Then, the scalar multiplication operation is defined as: $k \cdot P = P + . + . + \cdots . . P$ (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 sum of P and Q is represented as $P + Q = (x_3, y_3)$, which satisfies: $x_3 = \Upsilon^2 - x_1 - x_2 \pmod q$ and $y_3 = (\Upsilon(x_1 - x_3) - y_1) \pmod q$ and l is defined as

$$\Upsilon = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \mod q & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \mod q & \text{if } P = Q \end{cases}$$

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

4. The proposed protocol

The following phases are included in the suggested protocol:

4.1 Initialization phase

Vehicle-based digital twin ($Twin_i$) servers can be used as third parties or as public/private key generators. During the initialization phase, the following actions are taken:

- $Twin_i$ selects the non-singular EC as $E_q(a,b) : y^2 \equiv x^3 + ax + b \ (mod\ q)$.
- Takes g as G's group generator. Selects a random value $x \in Z_q^*$, which is Twin_i's secret key.
- Selects secure hash function.
- $Twin_i$ chooses random number $w \in Z_q^*$, set as a private key.

4.2. Registration phase

To obtain the data needed for communication with $Twin_i$, AV, and the DT-vehicular network. This is a detailed explanation of how to register for AV and $Twin_i$:

Step 1. AV input his/her identity ID_A and password PW_A, computes $R_1 = h(x \parallel PW_A \parallel ID_A)$ and sends $\{ID_A, PW_A, R_1\}$ to $Twin_i$ via secure channel.

Step 2. On receiving $\{ID_A, PW_A, R_1\}$, $Twin_i$ computes $R_2 = R_1 \oplus h(ID_T \parallel ID_A)$ and sends $\{R_2, ID_T, w\}$ to AV via secure channel.

Step 3. On receiving $\{R_2, ID_T, w\}$ from $Twin_i$, AV computes computes $R_3 = R_2 \oplus h(ID_T \parallel ID_A)$ and AV stores $\{R_3, w\}$ in database.

4.3 Login, authentication and key agreement phase

Upon registration, AV and $Twin_i$ authenticated each other and shared a secure session key to facilitate encrypted communication. This authenticated their credentials, maintained confidentiality and integrity of data, and avoided unauthorized access. The subsequent steps outline the secure login and authentication process forming a trusted communication session.

Step 1. AV login with ID_A^*, password PW_A^* and computes $R_1^* = h(x \parallel PW_A^* \parallel ID_A^*)$. Further, AV verifies $R_1^* ?= R_3$ if yes then AV generates $\xi \in Z_q^*$, computes $H_1 = h(w \parallel ID_A \parallel ID_T)$ and $K_1 = h(PW_A \parallel w)$. Then, AV encrypts $E_1 = E_{K_1}(\xi g, H_1)$ and AV sends $M_1 = \{E_1, t_1\}$ to $Twin_i$.

Step 2. On receiving $M_1 = \{E_1, T_1\}$, $Twin_i$ verifies $t_2 - t_1 \leq \triangle t$ aborts if not fresh, otherwise computes $K_1^* = h(PW_A \| w)$ and decrypts E_1 with K_1^* as $(\xi g, H_1) = D_{K_1^*}(E_1)$. Further, $Twin_i$ computes and verifies $H_1^* ? = h(w \| ID_A \| ID_T)$ If yes, then generates $\eta \in Z_q^*$ and computes session key as $SK_T = h(ID_T \| ID_A \| w \| \eta\xi g \| t_3)$, $H_2 = h(w \| H_1^* \| t_3)$ and $K_2 = h(K_1^* \| H_1^*)$. Finally, $Twin_i$ encrypts $E_2 = E_{K_2}(H_2, \eta g)$ and sends $M_2 = \{E_2, T_3\}$ to AV.

Step 3. On receiving M_2, AV first verifies $t_4 - t_3 \leq \triangle t$ if yes then computes the key $K_2^* = h(H_1 \| K_1)$ and decrypts $(H_2, \eta g) = D_{K_2^*}(E_2)$ with K_2^*. AV also computes and verifies $H_2? = h(w \| H_1^* \| t_3)$. If yes then, AV computes the session key $SK_A = h((ID_T \| ID_A \| w \| \xi\eta g \| t_3)$.

Finally, AV and $Twin_i$ agree for common session key $SK = SK_A = SK_T$ which will use for future communications via public channel.

5. Analysis of security of the proposed protocol

This section provides a critical evaluation of the suggested protocol's security aspects. To make it resilient to possible dangers, we have carried out both formal and informal study. The protocol strongly ensures the secrecy and safe authentication of the $Twin_i$ and AV parties. Our explanation of the security features and results is contained in the subsections below:

5.1 Man in the middle attack

As mentioned above, in the login an attacker could have sent some earlier messages which have been sent back in response from the server side itself, in a specific attack called Man in the Middle Attack. This method keeps an attacker away from computing with an actual entity with new random numbers and pseudonymous identities so that the attack is being prevented. Apart from this, the proposed framework is also immune to the attack because messages M_1 and M_2 are hashed by a hash function after they are encrypted using private keys for M_1 and secret key for M_2.

5.2 Private key security

The user selects a private key $k \in Z_q^*$ In order for an attacker A to break the security of the system, they would need to calculate the private key from information available to the general public. But as the private key is computed from a master key g, and as the ECC discrete logarithm problem is intractable, it is extremely difficult for an attacker to determine the private key. Since the attacker can do no other than fail in penetrating the system, we can confidently conclude with certainty that the security of the system holds good.

5.3 Session key disclosure attack

Under the given scheme, $Twin_i$ and every AV calculate a secret key during login, authentication and key agreement phase. Subsequently, the session key SK_A is calculated based on this key. It can be seen that all values required to calculate the session key are known publicly except ξ and η. Both $Twin_i$ and all AV share a common randomly chosen values of ξ and η. This session key SK_T would thus not be computable for the attacker if and when the attacker acquires secret key K_1 or K_2 due to its non-obtainable information required to determine values ξ and η in polynomial time. In addition, the newly introduced protocol utilizes a hash function for secure communication; as invertible hash functions do not exist, the attacker cannot derive SK from the discussed protocol. Thus, the newly introduced protocol is secure from the attacks leaking session keys.

5.4 Eavesdropping attack

An assault known as an eavesdropping attack is one that can stop communication by intercepting messages sent over an open channel. Our suggested methodology resolves this problem by generating a new random integer for every authentication cycle and determining all other parameters using a hash function. This technique will prevent the attacker from obtaining any user identities or parameters. Furthermore, the session key $SK = SK_A = SK_T$ cannot be determined, making it impossible for the attacker to calculate. Thus, there is strong protection against eavesdropping in our suggested method.

5.5 Denial of service attack (DoS)

The protocol's protective feature limits the number of login and authentication attempts to three in order to prevent DoS attacks. If an antivirus program fails to provide the required credentials after three tries,

its login and authentication features will be temporarily deactivated. This restriction ensures that the system is constantly available and functional and successfully thwarts (DoS attack.

5.6 Key freshness

The communication channel's security depends on the key's freshness. It is imperative that a new key be generated each time the compromised one is compromised to avoid future distorted connectivity. In order to ensure key freshness, we address this issue in our suggested method by employing a fresh random integer and timestamp at each stage of authentication.

5.7 Perfect forward secrecy

The suggested technique makes use of PFS to stop an attacker from deriving the session key $SK = SK_A = SK_T$. This is due to the fact that the session key does not contain the information about the prior key. The fresh random numbers chosen by $Twin_i$ and AV will be hard for the attacker to calculate, making it computationally impossible to obtain the value of $\xi\eta g \; or \; \eta\xi g$. Therefore, the protocol guarantees absolute forward secrecy; session keys are not compromised even if the private secret key is compromised.

5.8 AV and $Twin_i$ node traceability attack

The attacker uses authentication communications in the AV and $Twin_i$ node traceability attack to try and track down the AV and $Twin_i$. The proposed protocol overcomes this attack by using the encrypted parameters E_1 and E_2, a private key, a one-way hash function, and a new timestamp. In order to prevent traceability from becoming untraceable, our design ensures that the identities of the AV and $Twin_i$ stay confidential.

5.9 Replay attack

Replay attacks, in which a malevolent attacker attempts to transmit a message that has been intercepted, are prevented by the described protocol. To stop such attacks, the protocol does use the following defenses. It uses new timestamps, random numbers, and a secure hash function with $H_1, H_1^*, H_2\, H_2^*$ requirements. These safeguards guarantee that any relay attempt of a previously intercepted message would fail, making the described protocol immune to replay assaults.

5.10 Offline user identity prediction attack

This is an attack in which an attacker attempts to infer a user's identification from the messages that are communicated via an open channel. To prevent this attack, the proposed solution uses user ID_A to construct a password and private key that are extremely resistant. The suggested system's defense against offline user identity prediction attacks is significantly increased by this safeguard.

5.11 Insider attack

An adversarial tactic known as an insider attack occurs when an unauthorized person gains access to a system and uses it to obtain user credentials or other data in order to use them to log in to other services without authorization. Communications between AV and $Twin_i$ that are encrypted with private keys, securely kept, and only available to authorized users thwart this attack. Because security has been put in place, the strategy stops any intruder from using corporatized identities to retrieve sensitive data. As a result, the architecture is resistant to insider threats.

5.13 Mutual authentication

There are two parties which take part in the secret key establishment phase of the proposed protocol: $Twin_i$ and AV. During the registration process, every one of the $Twin_i$ nodes and every one of the AV nodes compute a common key. They, however, need to authenticate one another first to confirm that they are legitimate prior to accepting the common key. In addition, prior to going on to the rest of the secret key agreement phase, all three parties perform mutual authentication to make personal identification certain. Mutual authentication is thus a critical component of the system.

6. Performance analysis

We conducted a rigorous test of our suggested protocol against various suggested schemes from Yao et al. [15], Wu et al. [16], Kumar et al. [17], and Nandy et al. [18]. We compared and tested the difference in key performance indicators, communication cost, and computation cost. Testing was performed on an Intel Pentium ® CPU 2020 Model with 240 GHz speed and 64-bit core Ubuntu 18.04 OS. Like earlier protocols, our suggested protocols were coded in the relatively robust programming language, Python 3.6. For testing the suggested authentication protocol, we employed the widely used network simulator (NS3)

platform. In the subsequent subsections, we proceed by providing an overview of the performance and the numerical results obtained by each protocol.

6.1 Computation cost

In order to make a general comparison, we have presented a complete computation of the cost of computing between the proposed approach and existing techniques. To signify the time for various operations engaged in our computation, we employ T_h, T_{ecm}, T_{sym}, and T_{fe} corresponding to respective processes of the SHA2 computation for a one-way hash, elliptic curve cryptography algorithm points multiplication, symmetric key operation, and fuzzy extractor operation. It has been established in earlier research [19] that the time of computations for the fuzzy extractor and EC point multiplication is virtually similar. The time taken for XOR operation was fluctuating; hence, it is left out of the calculation. But these were the actual execution times 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 comparison of calculation steps to the authentication and communication steps as a car can be registered once. As our analysis indicates, the approach suggested by Wu et al. [16] requires $34T_h + 2\,T_{ecm} = 0.877812\,ms$. Yao et al. [15] need $22T_h + 7\,T_{sym} + 4\,T_{ecm} = 1.290448$ ms. Kumar et al. [17] also achieve the execution time of $10T_h + 5\,T_{ecm} = 0.69353\,ms$. Nandy et al. [18] have stated that the requirement is $13T_h + 2\,T_{sym} + 1T_{fe} = 0.48657$ ms. But during execution, our suggested method needs only $11T_h + 4\,T_{sym} = 0.470578\,ms$. From these comparisons, we can find that our suggested protocol has better computing efficiency. Figure 2 shows the comparison of the computation cost of the proposed protocol and related protocols.

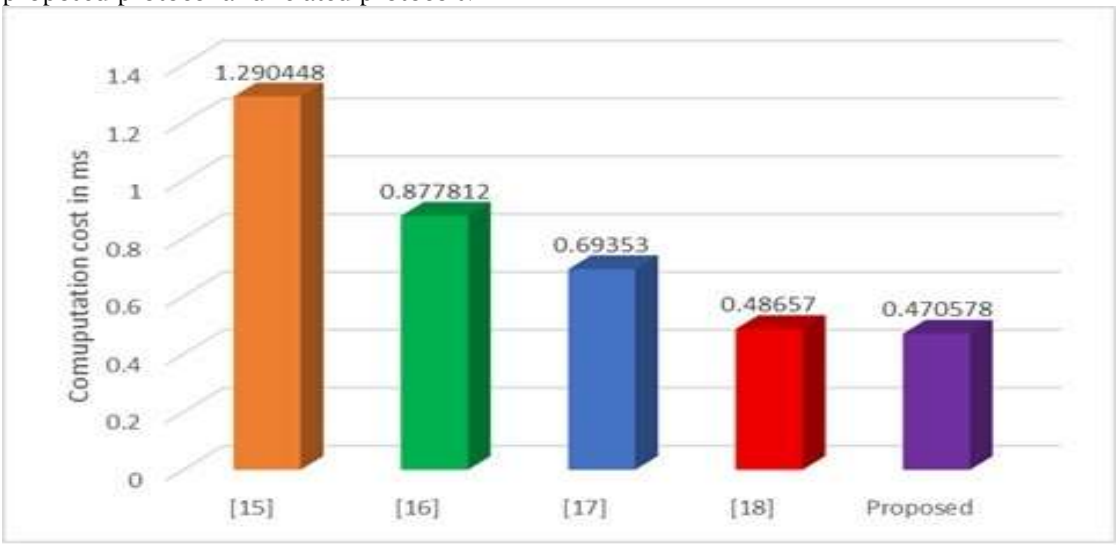

Figure 2: Computation cost comparison

7. CONCLUSION

This paper introduces a digital twin-based computation and data integration system for autonomous vehicles. The strategy includes synchronizing a digital twin with its physical counterpart to gather real-time required data and employing cloud computing for timely feedback. Synchronization allows efficient decision making and operation optimization. Verification protocols are introduced both in individual twins and among various twins to provide secure communication. Security analysis validates that the system is secure against different kinds of cyberattacks. Moreover, we compare our system with traditional ad hoc vehicular communication techniques and prove that our system provides better performance and efficiency. Performance evaluation and security validation results validate that our protocol fulfills critical security requirements such as data integrity, authentication, and confidentiality. In addition, it does all this at the cost of low computational and communication overhead. This makes the solution especially well-suited for real-time and resource-scarce vehicular environments. With these benefits, usage of the proposed approach is very much applicable in situations pertaining to digital twin technology within

intelligent transportation systems. Not only does it improve autonomous vehicle performance but also supports secure, scalable, and dependable vehicular cloud computing infrastructure.

REFERENCES

[1] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, Y. Liu, A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects, IEEE Internet of Things Journal (2023).
[2] 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.
[3] D. Parekh, N. Poddar, A. Rajpurkar, M. Chahal, N. Kumar, G. P. Joshi, W. Cho, A review on autonomous vehicles: Progress, methods and challenges, Electronics 11 (14) (2022) 2162.
[4] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, M. Hafeez, A survey of autonomous vehicles: Enabling communication technologies and challenges, Sensors 21 (3) (2021) 706.
[5] R. Roriz, J. Cabral, T. Gomes, Automotive lidar technology: A survey, IEEE Transactions on Intelligent Transportation Systems 23 (7) (2021) 6282–6297.
[6] C. He, T. H. Luan, R. Lu, Z. Su, M. Dong, Security and privacy in vehicular digital twin networks: Challenges and solutions, IEEE Wireless Communications (2022).
[7] S. S. Dhanda, B. Singh, P. Jindal, Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks, Journal of Interdisciplinary Mathematics 23 (2) (2020) 463–470.
[8] X. Luo, J. Wen, J. Kang, J. Nie, Z. Xiong, Y. Zhang, Z. Yang, S. Xie, Privacy attacks and defenses for digital twin migrations in vehicular metaverses, IEEE Network (2023).
[9] S. Kuutti, R. Bowden, Y. Jin, P. Barber, S. Fallah, A survey of deep learning applications to autonomous vehicle control, IEEE Transactions on Intelligent Transportation Systems 22 (2) (2020) 712–733.
[10] S. Khan, M. Farnsworth, R. McWilliam, J. Erkoyuncu, On the requirements of digital twin-driven autonomous maintenance, Annual Reviews in Control 50 (2020) 13–28.
[11] H. Alghodhaifi, S. Lakshmanan, Autonomous vehicle evaluation: A comprehensive survey on modeling and simulation approaches, IEEE Access 9 (2021) 151531–151566.
[12] S. M. Hossain, S. K. Saha, S. Banik, T. Banik, A new era of mobility: Exploring digital twin applications in autonomous vehicular systems, in: 2023 IEEE World AI IoT Congress (AIIoT), IEEE, 2023, pp. 0493–0499.
[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, RSFVC: Robust biometric-based secure framework for vehicular cloud networking, IEEE Transactions on Intelligent Transportation Systems, IEEE, 2023.
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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.