Journal of Robotics and Control (JRC)
Volume 6, Issue 2, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i2.25663

Secure and Efficient Mutual Authentication Protocol for VANETs Using Edge Computing and Signature-Based Cryptography

Abdulnasser AbdulJabbar Abbood [1], Faris K. Al-Shammri [2], Zainab Marid Alzamili [3], Mahmood A. Al-Shareeda [4*]
Mohammed Amin Almaiah [5], Rami Shehab [6], Md Asri Bin Ngadi [7], Abdulaziz Zaid A. Aljarwan [8]
[1, 4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq
[2] Biomedical Engineering Department, College of Engineering, University of Warith Al Anbiyaa, Karbala 56001, Iraq
[3] Education Directorate of Thi-Qar, Ministry of Education, Iraq
[4] Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq
[5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman 11942, Jordan
[6] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[7, 8] Faculty of Computer Science, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[8] Information Security Department, College of Computer Science and Engineering, University of Hail, Ha'il 81481, Saudi Arabia
Email: [1] abdulnasser.abbood@stu.edu.iq, [2] faris.kar@uowa.edu.iq, [3] Zainab.alzamili@utq.edu.iq,
[4] mahmood.alshareedah@stu.edu.iq and m.alshareeda@iuc.edu.iq, [5] m.almaiah@ju.edu.jo, [6] Rtshehab@kfu.edu.sa,
[7] dr.asri@utm.my, [8] abdulaziz.zaid84@gmail.com
*Corresponding Author

***Abstract*—Security in vehicular ad-hoc networks (VANETs) as a result, vehicular ad-hoc networks (VANETs) need to adopt and implement strong security protocols respective to vehicle-to-vehicle and vehicle-to-infrastructure communication. But state-of-the-art authentication methods have drawbacks like computational overhead, scalability issues, and susceptibility to identity stealing, replay attacks and data manipulation. To mitigate these issues, we present an innovative protocol for mutual authentication in edge computing assisted VANEts by employing an elliptic curve signature-based to improve the security and performance of the protocol. The proposed scheme guarantees low-latency authenticated by offloading computation tasks to edge nodes and simultaneously provides conditional privacy-preserving vehicle tracing for law enforcement. Formal security verification using ProVerif shows to be resilient towards replays, man-in-the-middle and eavesdropping attacks. Simulation results also show that the proposed protocol achieves highly efficient computational and communication overhead in comparison with current approaches. The performance results are promising and therefore, the proposed scheme can I be considered as practical and scalable for realistic applications in VANET.**

***Keywords*—Edge Computing; VANET; Mutual Authentication; Elliptic Curve; Vehicular Adhoc Networks**.

I. INTRODUCTION

Over the past decade and years, the Vehicular Ad Hoc Networks (VANETs) have been driven by the growing number of vehicular networks and the growing number of connected vehicles [1]–[3]. By allowing vehicles to communicate with each other (V2V) and with the roadside infrastructure (V2I) in real-time, VANETs help to increase road safety, efficiency of traffic and convenience of the drivers [4]–[6]. Nevertheless, the security vulnerabilities associated with these wireless communications are quite high, such as those involving identity spoofing, replay attacks, data tampering while in transit, eavesdropping, change, and interception [7]–[9]. By default, authenticating successful mechanisms and preventing various attacks can allow attackers to impersonate legitimate vehicles, inject false data, or disrupt the network, causing great safety and traffic hazards [10]–[12].

Vehicular ad hoc networks (VANETs) are crucial for bettering road conditions and the driving experience due to the proliferation of automobiles and advancements in wireless communication technology [13], [14]. Message authentication provides the foundation for secure communication in VANETs,

which are centred around vehicles communicating with each other. To make message authentication more efficient, several approaches have been developed. An on-board unit (OBU), a trusted authority (TA), and a roadside unit (RSU) make up a typical VANET architecture [3], [15]. Registration and issuance of secret key material are responsibilities of the TA, which functions as the trusted management centre. Installed at strategic points along roadways, RSUs connect automobiles to TAs. Communication between vehicles and infrastructure is controlled by the on-board unit (OBU) in each vehicle [16]–[18]. Without a proper security plan for VANETs, malevolent attackers can alter the message transmitted by a vehicle or even pose as a vehicle because V2V and V2I communications are wireless. The receiver of a communication in a VANET must, therefore, verify its authenticity and trustworthiness. The information contained in a message may only be trusted if the message itself is reliable [19]–[21].

A growing number of people are worried about privacy in VANETs these days. Nobody wants their personal details or driving route revealed [22], [23]. Accordingly, VANET communication protocols should meet anonymity requirements, which means that vehicles should interact with all entities using a fake identity rather than a genuine one [24], [25]. On the other hand, you should stay away from a totally anonymous programme for reasons like these. Although it is impossible to completely eliminate the possibility of malevolent vehicles sending fake communications or trying to alter legitimate ones, it is possible to track such vehicles and identify who they really are. We examine strategies in VANETs that can meet the conditional privacy-preserving (CPP) criterion [26]–[28].

A public key infrastructure (PKI) based signature authentication technique was presented by Raya and Hubaux [29] to address privacy and security concerns in VANETs. All traffic-related data transferred on VANETs must undergo authentication before it can be trusted, according to their methodology. Authentication and integrity checks are best handled by PKI-based systems [30]–[33]. Nevertheless, these plans do come with certain drawbacks. There is a direct proportional relationship between the number of vehicles and the RSU's gearbox overhead since each vehicle must keep a large number of pseudonym certificates [34], [35]. As a second point, a high volume of vehicles can cause communication channel congestion due to the relatively large size of certificates. In their schemes, the RSU and vehicles validate the received messages sequentially; this process is extremely inefficient and not fit for deployment in real-world circumstances [36]–[38].

An effective method for verifying the signatures of batches of messages in V2I communications was proposed by Zhang *et al*. [33] to solve the performance problems with PKI-based methods. The RSU in this method may verify many received messages simultaneously, which greatly reduces the total verification overhead and improves the operating efficiency of the VANETs. This is in contrast to prior schemes where each received message is confirmed individually. Additionally, their approach is highly favourable in terms of communication and computing cost, and there is no need for a certificate because it is based on identification. There have been numerous improvements to identity-based batch authentication techniques since Zhang's proposal [33], including [33] and [39]. While these schemes do increase efficiency, they aren't designed to handle situations where things aren't going according to plan, such when there are a lot of vehicles.

Most vehicles have limited processing capability, therefore it will take longer than expected to verify several messages. Chim *et al*. [40] offered a solution to these issues by having the RSU assist adjacent vehicles in verifying the received messages, eliminating the requirement for those vehicles to do it independently. Specifically, the RSU executes batch authentication on a number of communications to ensure their authenticity. The validity of the messages in the batch is determined by the success of the batch authentication. If not, then at least one message is invalid, and to identify them, batch authentication and a binary search would be carried out. Upon verifying the authenticity of the vehicle-sent messages, the RSU would next configure two bloom filters to save the authentication outcomes. One specific usage of the RSU is to create a positive filter for valid message hashes and a negative filter for invalid message hashes. After that, at a predetermined frequency, the RSU would transmit the positive and negative filters to vehicles in the area. Therefore, in order for the cars to confirm the messages, they would just need to check the two filters. The overall system efficiency is enhanced, and the amount of duplicated authentication is substantially reduced, thanks to this. Nevertheless, it would be overloaded if its performance were entirely dependent on the RSU's computational capabilities [35], [41].

By showing that adjacent vehicles may share the computing load on the RSU, Liu *et al*. [42] made it possible to fully utilise the computational capabilities of vehicles. Based on the computing power, the system chooses proxy vehicles in this approach. When the RSU verifies a message, the proxy vehicles should relay that information to the RSU along with their findings. The accuracy of the outcome will then be verified by the RSU. Even while the suggested method greatly enhances the RSU's verification performance, it still falls short due to the basic operation's heavy reliance on bilinear pairing and map-to-point. Furthermore, the RSU does not verify if the original signature is faulty or if the proxy vehicle altered the valid signature in the event that a batch of communications includes defective messages, meaning that the signature of a message is invalid.

Most data generated between the VANETs' (vehicles') periphery and the cloud's periphery are inefficient, just like the VANETs themselves [43]. Edge computing has been implemented to address this issue. Instead of limiting computation

to the cloud data centre, a method known as "edge computing" enables computation to take place at the network's periphery, near the data source [44]. The most distinctive feature of edge computing is the fact that the very edges of the network are both data consumers and producers. In contrast, the network's periphery only serves as a consumer in cloud computing. We present an innovative edge-computing approach to VANET message authentication in this research. Our plan calls for the RSU to serve as the car's cloud, while another component of the vehicle will serve as an edge-computing node to help authenticate messages. The following are some of the contributions we provide in this paper to overcome the aforementioned drawbacks:

Based on the shortcomings of previous proposals for VANET authentication, we present a new mutual authentication protocol that incorporates edge computing and signature-based cryptography to achieve improved levels of security, efficiency, and scalability. - A summary of key contributions of this work are as follows:

- The optimal edge-assisted mutual authentication The introduction of signature-based authentication mechanism of edge nodes to delegate tasks reduces the latency and computational overhead of vehicles and RSUs.
- Common Attack Resistance: The protocol resists the identity spoofing, replay attacks, eavesdropping, and man-in-middle attacks.
- Privacy-Preserving Vehicle Tracking: Our scheme offers conditional privacy by allowing authorized entity such as law enforcement, to trace vehicle identities when needed while ensuring that the personal information is not disclosed to any unauthorized third party.
- Security Analysis: We analyze our protocol using a formal security verification tool ProVerif, proving that our solution is secure against standard cryptographic attacks.
- We demonstrate lower computational and communication costs of our approach as compared to existing VANET-based authentication schemes via simulations and performance analysis, to highlight the practical scalability of our proposed design for real-world implementation.

The rest of this paper is structured as follows. Section II reviews security approaches on VANET. Section III introduces architecture of design model based on our solution. Section IV proposes novel work of this paper. Section V evaluates informal and formal verification process of the proposal. Section VI shows results of costs in terms of computation and communication. Lastly, the concluation and future work of this paper are summarized in Section VII.

II. Related Work

Some related works [45]–[52] proposed to provide security and privacy in VANET. Lim *et al*. [53] presented a key management approach that was both efficient and effective for group signature based authentication. This protocol allowed for the extension of groups to domains with many roadside units. In addition to delivering group keys to vehicle nodes in a secure manner, their approach guarantees security characteristics. With the aim of enhancing the efficiency and security of cross-region vehicle authentication, Zhang *et al*. [54]presented a modular and decentralised system. Upon entering a new region, the cross-region vehicle can choose the edge computing vehicle by checking the reputation value of the nearby cars. Goudarzi *et al*. [55] designed a mutual authentication approach based on Quotient Filter (QF) and fog computing by assigning unique pseudonym and ECC to maintain anonymity and achieve message authentication in VANET system, receptively. Tahir *et al*. [56] proposed a secure and efficient data transmission across an open channel that is possible with the help of this work's multi-factor authenticated key agreement technique for VANETs, which is both lightweight and encrypted. Almazroi *et al*. [57] proposed a technique based on the Chebyshev polynomial to safeguard vehicle-to-vehicle communication in 5G-based vehicular networks from DDoS attacks. This proposed used the semi-group and chaotic properties of the Chebyshev polynomial. To address these concerns in 5G-enabled car networks, Al-Mekhlafi *et al*. [58] suggested a CPPA approach that relies on fog computing (FC). Their proposal the FC-CPPA technique, which involves preloading each legitimate vehicle with a set of public anonymity identities and their associated signature keys obtained from a fog server. Almazroi *et al*. [59] proposed the L-CPPA system that uses a fog server to produce secret keys, which are then sent to each registered automobile via a 5G-Base Station (5G-BS). The suggested L-CPPA approach has the trusted authority, not the vehicle's Onboard Unit (OBU), keep track of the master secret information for each fog server. Manivannan *et al*. [46] proposed a privacy-protecting, lightweight authentication protocol that uses exclusively hash functions and exclusive-OR operations, inside an appropriate communication paradigm for VANET. To ensure that only authorised vehicles can access the services provided by zones, Chen *et al*. [60] presented BASRAC, a rule-based access control and batch authentication mechanism for VANETs. Additionally, BASRAC allows for batch verification, which boosts authentication efficiency even further. Wang *et al*. [61] designed lightweight authentication mechanism that once the initial mutual authentication with the closest roadside unit (RSU) was completed, their methodology allows EVs to proceed with the mutual identity authentication with subsequent RSUs without having to redo the tedious calculations. Gupta *et al*. [62] proposed a new framework for an Internet of Vehicles (IoV) architecture model and an authentication-based protocol (A-MAC) for smart vehicular communication. In order to keep communications secure while they are being sent between cars, the method employs cryptographic principles and hash operations. Ouaissa *et al*. [63] designed secure mutual authentication by combining vehicular ad-hoc networks with Fifth-Generation (5G) networks

due to the diverse range of applications and services that are needed by vehicle networks. Soleymani *et al*. [64] offered a new framework for an Internet of Vehicles (IoV) architecture model and an authentication-based protocol (A-MAC) for smart vehicular communication. To ensure the necessary level of security, the technique employed cryptographic principles to transmit messages between cars and employs hash operations. An innovative group signature-based approach was suggested by Wang *et al*. [50] for mutual authentication between vehicle-to-vehicle (V2V) communication in a 5G-enabled VANET's hybrid D2D message authentication (HDMA) scheme. An improved and more secure group of vehicles based on the Key Agreement Protocol (KAP) was proposed by Nyangaresi *et al*. [65] for use in 5G networks. In this case, Automated Validation of Internet Security Protocols and Applications was used to validate the security results. Asghar *et al*. [66] offered a mechanism that streamlines the authentication process and makes CRL size linear. Meanwhile, Asghar *et al*. [66] simulated a variety of authentication queries to demonstrate the decreased time. Tangade *et al*. [67] proposed privacy-preserving authentication (DSPA) method for safe vehicular ad hoc networks was both decentralised and scalable. A mixed cryptography was used by the suggested scheme. When communicating between vehicles and infrastructure, DSPA uses symmetric hash message authentication code (HMAC) authentication, and when communicating between vehicles, it used asymmetric identity-based (ID-based) cryptography. Cao *et al*. [68] presented a new group signature protocol for VANET authentication that combines lattice cryptography for quantum-resistant authentication with Bonsai-tree signature architecture for forward security. Yue *et al*. [69] offered a new authentication protocol technique that uses the entire sub-tree method to accomplish membership revocation, which guarantees forward security. By dividing the VANET domain into multiple sub-regions, Sun *et al*. [70] can implemented a distributed key management (DKM) method that ensures all vehicles regularly update their group secret key with the regional group manager in charge of their respective region. Zhang *et al*. [71] offered a smart drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad hoc networks to let vehicles communicate more efficiently while protecting their privacy. An efficient authentication scheme that preserves privacy was proposed by Tian *et al*. [72]. Despite the limited resources of small-scale UAVs, their approach guarantees efficient authentication through the use of a lightweight online/offline signature design. Khalid *et al*. [73] designed an anonymous handover authentication system to safeguard the flight path of drones by providing secure key management, rapid verification, and signature creation. Lee *et al*. [74] suggested a simple strategy for managing regional segmentation and resolving overhead based on the dynamic characteristics of vehicles. Our protocol also employs mutual authentication and honey list technology to safeguard vehicle information during transmission over public channels, which might be vulnerable to many types of assaults. In order to set up a secure connection between devices and the cloud through the movable drone, Mall *et al*. [75] initially created a lightweight protocol and an appropriate architecture based on Physically Unclonable Function (PUF) for the endeavour, which is employed for communication message encryption. To effectively aid and guarantee the privacy and security of maritime transportation systems, Chaudhry *et al*. [76] offered a lightweight authentication protocol that can be used with 6G-IoT. To simplify the verification of digital signatures and provide conditional privacy protection in VANET communications, Samra *et al*. [77] presented a novel system called Certificateless Aggregate based on Traceable Ring Signature (CLA-TRS).

III. Design Model Architecture

This strategy takes into account four individuals. You have TA, the RSU, the edge computing, and the car. In the phases of message transmission and vehicle identification revelation, after TA registrations, RSUs, edge computing, and cars engage in communication and session formation. Edge server act as go-betweens for vehicles and RSUs, and the two types of channels in question are wireless. The connection between RSU and TA is electrical. Allotting parameters and keeping tabs on cars are TA's responsibilities. General data transmission does not involve it. It is clear that TA is solely used during the registration and vehicle identity disclosure processes. No data held in any entity is considered vulnerable to breaking. Every communication between entities is vulnerable to interception, forgery, or blocking by the enemy. Conversely, we might state that the attacker has channel control during the message transmission and vehicle identification revelation stages. Fig. 1 clearly shows the data flow and architecture, which everyone can read and comprehend.

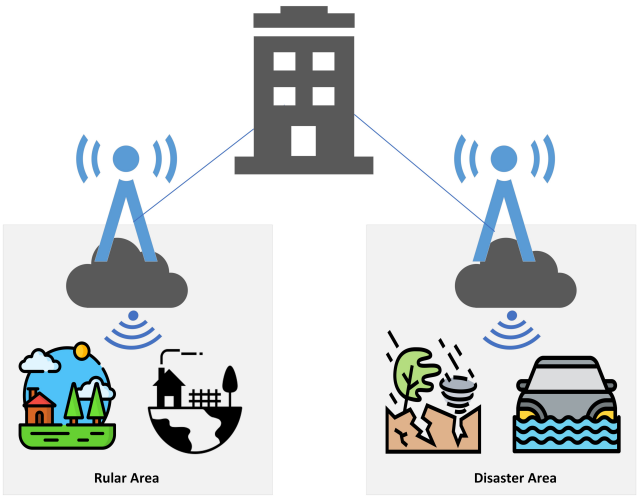

Fig. 1. System model for our design model

IV. The Proposed Scheme

This proposes have the following stages called, setup, enrollment, mutual authentication, and vehicle identity disclosing. Table I contains the referenced annotations.

TABLE I. General Utilised Notations

Notations	Definition
P	Generator point on elliptic curve
q	Large prime number (order of P)
G	Cyclic additive group on an elliptic curve
TID	True identity of vehicle or RSU
x_A, Pub_A	Private key and public key of the trusted authority (TA)
AID_i	Anonymous identity of a vehicle
h	Secure hash function
m_i	Message exchanged about road conditions
$H_1, H_2, H_3, \ldots$	Cryptographic hash functions used for different security operations
$\oplus$	XOR operation

A. Setup

This phase initializes the system parameters as follows.

- TA uses a point generator P and a big prime order q to create a cyclic additive group G on an elliptic curve.
- TA pick ups as TID_A identity, x_A as its private key, and $Pub_A = x_A \cdot P$ as its public key.

B. Enrollment

This phase is responsible for enrolling the components in the system as follows.

1) RSU Enrollment: For each RSU, TA assigns TID_r as its identity, x_k as private key, and $Pub_x = x_k \cdot P$ as public key. Then TA submits these parameters to RSU through the secure channel.

2) Edge Computing Enrollment: For each edge computing, TA assigns TID_e as its identity. For each RSU, TA computes $\beta_j^x = H_1(TID_r||x_A||TID_e)$ and transmits TID_r, Pub_r all of β_j^x to edge computing through the channel security.

3) Vehicle Enrollment: For each vehicle, TA assigns TID_v as its identity. For each RSU chooses $x_i \in Z_q^*$ and anonymity-ID $AID_i \in 0, 1^s$, computes $\beta_i^x = H_2(AID_i||x_i||TID_r)$, $\alpha_i^x = H_3(TID_x||x_k)$, $s_i^k = c_i + H_4(TID_r||TID_A||Pub_A)c_k$, and $f_i = x_i \cdot P$, and then transmits AID_i, β_i^k, α_i^k, s_i^k and d_i to vehicle through a channel security. TA saves (TID_v, f_i) in its databases.

C. Mutual Authentication

- Edge computing is set in RSU' communication range, and it sends TID_j, TID_k and Pub_k periodically.
- Vehicle V_i generates the information m_i. Once obtaining the periodical transmission. Vehicle chooses $e_{i,1} \in Z_q^*$ and $AID_i^{new} \in \{0,1\}^x$, selects the timestamp t_i, computes $A_{i,1} = e_i \cdot P$, $A_{i,2} = \beta_i^x \oplus H_4(AID_i||e_{i,1 \cdot Pub_k||t_i}) \oplus (f_i)_s$, $A_{i,3} = AID_i^{new} \oplus H_6(AID_i||e_{i,1}||f_i||e_{i,1}||t_i) \oplus m_i$, $A_{i,4} = \alpha_i^k \oplus H_7(AID_i||AID_i^{New}||f_i||r_{i,1}||t_i) \oplus m_i$, $A_{i,5} = e_{i,1} + H_8(AID_i||AID_i^{New}||f_i||Pub_k||A_{i,1}||e_{i,1}Pub_k||m_i||t_i)S_i^k$, $A_{i,6} = H_9(AID_i||m_i||TID_r||e_{i,1}Pub_a) \oplus TID_i$, $A_{i,7} = e_{i,1} + H_{10}(AID||TID_i||r_{i,1}Pub_a||B_{i,1}||Pub_a)s_i$, and transmits $M_1 = \{AID_i, A_{i,1}, A_{i,2}, A_{i,3}, A_{i,4}, A_{i,5}, A_{i,6}, A_{i,7}, t_i\}$ to edge computing.
- Once abating M_1, D chooses $e_2 \in Z_q^*$ and gets the position information Pos_j, calculates $A_{j,1} = e_2 \cdot P$, $A_{j,2} = b_j^k \oplus H_1 1(e_2 Pub_k||t_i) \oplus Pos_j$ and $A_{i,3} = H_1 2(A_{j,1}||Pub_k||e_2 Pub_k||t_i||\beta_j||TID_j||TID_r||M_1)$, and transmits $M_2 = M_1, A_{j,1}, A_{j,2}, A_{j,3}, TID_j$ to RSU.
- RSU verifies t_i after obtaining M_2, and calculates $A_{k,1} = x_k A_{i,1}$, and $A_{k,2} = A_{i,2} \oplus H_2(AID_i||x_k||TID_r) \oplus H_5(TID_i||A_{k,1}||t_i)$. Then f_i can be deduced. Then RSU passes to calculates $AID_i^{new} = H_6(AID_i||A_{k,i}||t_i||TID_e||TID_r) \oplus A_{i,3}$, $m_i = A_{i,4} \oplus H_4(TID_k||x_k) \oplus H_7(TID_i||A_{k,1}||t_i||TID_j||TID_e)$ and verifies if $A_{i,5} = B_{i,1} + H_8(TID_i||TID_i^{new}||f_i||Pub_i||A_{i,1}||A_{K,1}||m_i||t_i)(d_i + H_5(TID_r||TID_A||Pub_k)Pub_k)$. M_1 can be considered from V_i if the verification methods. Once RSU obtains multiple information from edge computing in a short period, it could process the batch verification as below.

$$\sum_{i=1}^{n} A_{i,5}P = \sum_{i=1}^{n} B_{i,1} + \sum_{i=1}^{n} H_8(AID_i||AID_i^{new}||f_i||Pub_k||A_{i,1}||A_{k,1}||m_i||t_i) \times (f_i + H_5(TID_s||TID_A||Pub))Pub_k \quad (1)$$

- RSU calculates $A_{k,3} = x_k A_{j,1}, Pos_j = A_{j,2} \oplus H_1(TID_j||x_k||TID_k) \oplus H_1 1(A_{k,3})||t_i)$ and tests if $A_{j,3} = H_{12}(A_{j,1}||Pub_k||A_{k,3}||t_i||H_1(TID_j||x_s||TIDr)||Pos_j||TID_j||TID_r||M_1)$. If ok, the entire information M_2 is legal.
- RSU selects timestamp t_s calculates $A_{k,4} = H_2(AID_i^{new}||x_k||TID_k) \oplus H_{13}(AID_i||AID_i^{new}||B_{i,1}, Pub_k||A_{A,1}||t_k)$ and $A_{k,6} = H_1 5(AID_i^{new}||AID_i||H_2(AID_i||x_k||TID_j||TID_e||A_{i,1}, A_{i,2}, A_{i,1}|TID)$ and transmits $M_3 = \{A_{k,4}, A_{K,5}, A_{k,6}, t_k\}$ to edge computing.
- Once obtaining M_3, edge computing verifies of t_k and if $A_{k,5} = H_1 4(TID_e||TID_k||t_k||Pos_k||A_{j,1}||e_2 Pub_k||A_{k,4})$. If ok, $M_4 = \{A_{k,4}, A_{k,6}, t_k\}$ is sent to Venice.
- Finally, vehicle verifies t_k and calculates $\beta_i^{new} = A_{k,4} \oplus H_{13}(AID_i)||AID_i^{new}||A_{i,1}||Pub_k||e_{i,1}||TID_j||TID_e||A_{i,1}||A_{i,7}, Pub_k||e_{i,1}, t_k||\beta_i^{new}$.

D. Vehicle Identity Disclosing

Government agencies like the police can disclose automobiles by taking these steps:

- RSU selects $r_3 \in Z_q^*$, computes $B_{k,7} = r_3 P$, and $A_{k,8} = H_{16}(A_{k,7}||r_3 Pub_a) \oplus m_i$, and transmits $m_5 = \{AID_i, A_{i,1}, A_{i,7}, A_{k,8}, TID_k\}$ to TA.

- TA selects Pub_k according to TID_k, computes $A_{A,1} = x_a A_{k,7}, B_{a,2} = x_a A_{i,1}$, $m_i = A_{k,8} \oplus H_{16}(A_{k,7}||A_{A,1})$, and $TID_i = A_{i,6} \oplus H_9(AID_i||m_i||TID_k||A_{A,2})$. TA check f_i according to TID_i and verifies if $B_{i,7}P = B_{i,1}(AID_i||TID_i||A_{a,2}||A_{i,1}||Pub_a)(f_i + H_4(TID_A||TID_i||TID_k||Pub_A)Pub_A)$. If ok, the above information is valid.

V. Security Analysis

A. Informal Security Analysis

- Confidentially: The personal information m_i is protected by $H_7(AID_i||AID_i^{new}||f_i||e_{i,1}pub||t_i)$ and k_i for messages M_1 and M_2. Answering $e_{i,1}pub$ refers running out the problem of Diffie–Hellman based on $A_{i,1} = f_i P$ and the public key of RSU pub. Therefore, there is no risk of attacks on the instant data.
- User anonymity: In both M_1 and M_2, TID_i is concealed by $H_9(PID_i||m_i||TID_i||d_iP||)$ in A_6. You also need d_i and Pub. The Diffie-Hellman problem is still a problem for the adversary.
- Unlinkablity: One important security aspect of an authentication protocol is its unlinkability, which means that an attacker cannot connect messages from two sessions that were started by the same entity. $A_{i,1} = d_1P$ and $A_{i,2} = d_2P$ vary from one session of our scheme to the next. The two strings are used to calculate other elements such as $A_{i,1}$, $A_{i,2}$, etc. That the messages will remain distinct and that the adversary will be unable to connect any two sessions is ensured by using such diverse random elements. The usage of $A_{k_7} = d_3P$ to compute other elements in the vehicle identity revelation phase further distinguishes M_5 from the others.
- Traceability: In the event that a vehicle engages in malevolent behaviour, the conditional traceability function of the TA may allow it to identify the vehicle. If specific government agencies want us to, TA can figure out the unique identification of the special vehicle. The other three plans, however, do not include this feature.
- Modify Attack Resistance: In our design, the Diffie-Hellman problem is a loving parent to every message. As an example, in order to change d_i, a will need to consider the calculations of both d_iPub_i and d_iPub_k in order to accommodate all hash functions. The other messages follow the same pattern.
- De-synchronization Attack Resistance: When a previously formed session's updated parameter is not received by any entity, a de-synchronization happens. Nevertheless, our work solely relies on strings stored in vehicles rather than RSUs, as there is no string that requires variation across sessions. You won't find inconsistencies in the data stored in RSUs and cars. Consequently, there will be no de-synchronization assault.
- Replay Attack Resistance: The messages include timestamps t_i and ts_i in our scheme. The receiver will reject the message because of the wrong timestamp if the enemy replays even a single message. This would allow us to prevent replay attacks.

B. Security Comparison

In Samra *et al*. [77], the cars and the RSU generate a ring signature. Unfortunately, the approach is unable to preserve this quality because the instant data is transmitted in plaintext. Since data can only go in one way under the technique described in [77], it is unable to provide reciprocal authentication. However, in the authentication technique proposed by Mall *et al*. [75], such identification is revealed in the public channel. The transfer of elements in Samra *et al*. [77] is limited to those pertaining to signatures. Instead of using conditional tracking, it is recommended to verify the vehicle's identify every time according to [75], [76].

We conclude that the UAV is defenceless against this assault because, as mentioned in [76], it cannot update its pseudo-identity or remain consistent with the altitude platform system if the fourth message is either blocked or lost.

C. Formal Verification

The security of cryptographic systems can be checked with the well-known tool Proverif [78]–[84]. It processes fundamental components, such as the Diffie-Hellman key agreement and the public key mechanism, under the conditions of the Dolev-Yao model. The scheme simulation code's outputs reveal the security status of the secret elements. Proverif offers an unlimited number of sessions in the simulation. Specifically, we rely on this well-liked instrument to do the official validation. Fig. 2 shows findings from our procedure.

```
Verification Summary
Query Secret dil_1, dil is true.
Query Secret d2 is true.
Query Secret  AIDNew_1, AIDNew is true.
Query Secret TIDi_1, TID_i is true.
Query Secret x_1, x  is true.
Query event (ev4) ==> event (ev3)  is true.
Query event (ev3) ==> event (ev2)  is true.
Query event (ev2) ==> event (ev1)  is true.
```

Fig. 2. Findings from our procedure

VI. Results

Performance evaluation and comparison with analogous protocols, such as those proposed by Mall *et al*. [75], Chaudhry *et al*. [76], and Samra *et al*. [77], is the goal of this section.

A. Implementation Environment

In this paper, the following symbols are measured using the MIRACL library [85] running on Ubuntu 20.04, i5–9400 CPU-based quad-core, and 16 GB RAM.

- T_{pb} refers the time cost of bilinear pairing.
- T_{sm} refers the time cost of scalar multiplication.
- T_{se} refers the time cost of symmetric encryption.
- T_h refers the time cost of hash function.
- T_{pa} refers the time cost of point addition.
- T_{mi} refers the time cost of multiplication inversion.

Table II displays the values of all these operations when implemented. The order of the applied elliptic curve group is 160 bits long, which is the same as the multiplication group, in terms of the parameters for communication cost. However, 1024 bits is the length of the second set. Two-way encryption using AES-128 and hash function using SHA2-256 were both executed in the test. The important aspect of message submission is taken into account here.

TABLE II. GENERAL UTILISED NOTATIONS

Notations	Time(ms)
T_{pb}	2.7325
T_{sm}	0.39865
T_{se}	0.025678
T_h	0.00423
T_{pa}	0.00246
T_{mi}	0.0852

B. Computation Costs

This part evaluates the computation cost of the proposal and other works, as shown in Table III and Fig. 3. The vehicle in scheme of Mall *et al*. [75] needed six hash functions and single symmetric encryption operation, which the whole process is $6T_h + T_{se}$ = 0.051058 ms. By operating drone component, the proposal needed ten hash functions and three symmetric encryption operations, which the whole process is $10T_h + 3T_{se}$ = 0.145012 ms. By operating RSU component, the proposal needed six hash functions and two symmetric encryption operations, which the whole process is $6T_h + 2T_{se}$ =0.076736 ms.

The vehicle in scheme of Chaudhry *et al*. [76] needed three hash functions and three symmetric encryption operations, which the whole process is $3T_h + 3T_{se}$ = 0.089724 ms. By operating drone component, the proposal needed hash function and two symmetric encryption operations, which the whole process is $T_h + 2T_{se}$ = 0.055586 ms. By operating RSU component, the proposal needed seven hash functions and eight symmetric encryption operations, which the whole process is $7T_h + 8T_{se}$ =0.235034 ms.

The vehicle in scheme of Samra *et al*. [77] needed two multiplication inversion operations, two scalar multiplication operations, point addition operation and four hash functions, which the whole process is $2T_{mi}+2T_{sm}+T_{pa}+4T_h$ = 0.98708 ms. By operating RSU component, the proposal needed two hash functions and bilinear pairing operation, which the whole process is $2T_h + T_{pb}$ = 12.74096 ms.

The vehicle in the our solution needed eight hash functions and two scalar multiplication operations, which the whole process is $8T_h + 2T_{sm}$ = 0.83114 ms. By operating edge component, the proposal needed hash function and scalar multiplication operation, which the whole process is $T_h + T_{sm}$ =0.40288 ms. By operating RSU component, the proposal needed twelve hash functions and four scalar multiplication operations, which the whole process is $14T_h + 4T_{sm}$ =1.65382 ms.

In Fig. 3, we compare the computation costs for various schemes such as Mall *et al*., Chaudhry *et al*., Samra *et al*., and the proposed model. Different Schemes will have different communication costs as shown in the Fig. 3 between the Nodes, Edge/Drone and RSU. This visualization enables a direct comparison of performance between different methodologies.

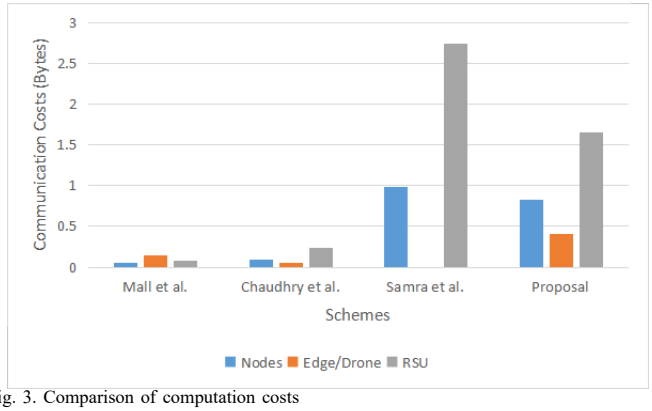

Fig. 3. Comparison of computation costs

C. Communication Costs

This part evaluates the communication cost of the proposal and other works, as shown in Table IV and Fig. 4. The single and multiple communication costs of proposed by Mall *et al*. [75] are 548 and 548 n, respectively. The single and multiple communication costs of proposed by Chaudhry *et al*. [76] are 977 and 977 n, respectively. The single and multiple communication costs of proposed by Samra *et al*. [77] are 140 and 140 n, respectively. The single and multiple communication costs of our work are 772 and 772 n, respectively.

The computation costs (in Bytes) across various schemes are shown in Fig. 4. Chaudhry *et al*. is the heaviest, with a cost of 977 bytes. Samra *et al*. achieves the smallest memory footprint: 140 Bytes and works quite efficiently. Mall *et al*. (548 Bytes) and the proposed approach (772 Bytes) fall somewhere in between them–achieving an acceptable trade-off between memory savings and functionality. The results in turn illustrate trade-offs between computational efficiency, and potential security or performance implications across the different designs.

TABLE III. COMPUTATION COSTS COMPARISON

Schemes	Nodes	Edge/Drone	RSU
Mall *et al.* [75]	$6T_h + T_{se}$ = 0.051058	$10T_h + 3T_{se}$ = 0.145012	$6T_h + 2T_{se}$ =0.076736
Chaudhry *et al.* [76]	$3T_h + 3T_{se}$ = 0.089724	$T_h + 2T_{se}$ =0.055586	$7T_h + 8T_{se}$ =0.235034
Samra *et al.* [77]	$2T_{mi} + 2T_{sm} + T_{pa} + 4T_h$ = 0.98708	-	$2T_h + T_{pb}$ = 2.74096
Proposal	$8T_h + 2T_{sm}$ = 0.83114	$T_h + T_{sm}$ =0.40288	$14T_h + 4T_{sm}$ =1.65382

TABLE IV. COMMUNICATION COSTS COMPARISON

Schemes	Single Message (Bytes)	Multiple Messages (Bytes)
Mall *et al.* [75]	548	548 n
Chaudhry *et al.* [76]	977	977 n
Samra *et al.* [77]	140	140 n
Proposal	772	772 n

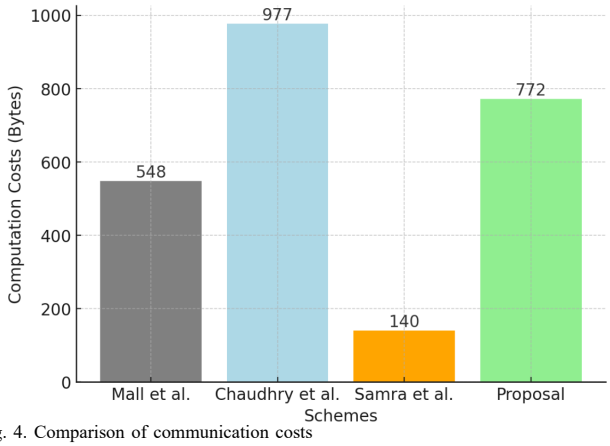

Fig. 4. Comparison of communication costs

VII. CONCLUSION AND FUTURE WORK

We proposed a secure and efficient mutual authentication protocol for VANETs that uses signature-based cryptography and edge computing to improve both security and performance. Our approach uses elliptic curve cryptography (ECC) and secure hash functions to accomplish authentication, cutting the computational overhead for vehicles yet providing strong guarantees. With the aid of validation mechanisms in the Roadside Unit (RSU), authentication messages in our protocol are processed as quickly as possible to avoid delay. The system also includes conditional privacy-preserving tracking, allowing law enforcement agencies to know vehicle identities only when they have reason for doing so. We seek a synthesis of user privacy and accountability

We have verified the security of our method by using ProVerif, showing that it can withstand all common attacks such as replay attacks, man-in-the-middle attacks and eavesdropping. Furthermore, grand simulations illustrate that our protocol has less computational overhead and communication costs than existing VANETs authentication schemes. In particular, batch authentication avoids some redundant verification operations which makes this method is great for real-world VANET applications, with a high price at LOS cost.

Naturally, though there are many positive features of this method, there are certain limitations too. The RSU's role in batch verification, while improving efficiency overall, does raise the computational overhead there. Indeed, to succeed in large-scale networks, more work will be needed. Moreover, although our protocol performs well with varying network conditions, more research is required: it should be tested in extremely high-density environments in order assess fully whether or not such systems can expand successfully.

Additionally, in order to increase both its security and performance, there are aspects of future research we might like to take up. One thing is for certain: now that quantum computing means traditional cryptographic methods can no longer be relied upon, we must look at post-quantum cryptographic techniques. For example we propose lattice based authenticating schemes for VANET. What kind of mechanism can ensure that these large-scale id systems will not be corrupted over the entire life cycle? Block chain technology makes it possible to decentralized identity management in vehicular networks. This lowers the all-permeating trust on a single center and increases the transparency of information. Nevertheless, facing the high likelihood that blockchain may be the proverbial elephant in a sugar bowl, we need to find insight into how to tailor lightweight consensus mechanisms for VANET. Enfin, we will optimize the computation model and AI-driven authority optimization of RSU processing efficiency to ensure it can adapt in real time within highly dynamic vehicle environments.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU250866)

REFERENCES

[1] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in vanets: a review of current research and future directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024, doi: 10.1145/3656166.

[2] I. A. Kapetanidou, P. Mendes and V. Tsaoussidis, "Enhancing Security in Information-Centric Ad Hoc Networks," *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-9, 2023, doi: 10.1109/NOMS56928.2023.10154444.

[3] A. Dutta, L. M. Samaniego Campoverde, M. Tropea, and F. De Rango, "A comprehensive review of recent developments in vanet for traffic, safety & remote monitoring applications," *Journal of Network and Systems Management*, vol. 32, no. 73, 2024, doi: 10.1007/s10922-024-09853-5.

[4] G. Liu, H. Li, J. Le, N. Wang, Y. Liu and T. Xiang, "LRCPA: Lattice-Based Robust and Conditional Privacy-Preserving Authentication for VANETs," in *IEEE Transactions on Vehicular Technology*, 20224, doi: 10.1109/TVT.2024.3485671.

[5] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions," *Electronics*, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203330.

[6] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar and M. A. Al-shareeda, "Performance Analysis of QoS in MANET based on IEEE 802.11b," *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pp. 1-5, 2020, doi: 10.1109/INOCON50539.2020.9298362.

[7] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, 2025, doi: 10.63180/jcsra.thestap.2025.1.4.

[8] A. Souri, M. Zarei, A. Hemmati, and M. Gao, "A systematic literature review of vehicular connectivity and v2x communications: Technical aspects and new challenges," *International Journal of Communication Systems*, vol. 37, no. 10, 2024, doi: 10.1002/dac.5780.

[9] A. K. Sangaiah, A. Javadpour, C.-C. Hsu, A. Haldorai, and A. Zeynivand, "Investigating routing in the vanet network: Review and classification of approaches," *Algorithms*, vol. 16, no. 8, 2023, doi: 10.3390/a16080381.

[10] S. Jiang, X. Zhu and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193-2204, 2016, doi: 10.1109/TITS.2016.2517603.

[11] P. K. Pandey, V. Kansal, and A. Swaroop, "Pki-smr: Pki based secure multipath routing for unmanned military vehicles (umv) in vanets," *Wireless Networks*, vol. 30, no. 2, pp. 595–615, 2024, doi: 10.1007/s11276-023-03503-5.

[12] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12–21, 2025, doi: 10.63180/jcsra.thestap.2025.1.2.

[13] R. Almutairi, G. Bergami and G. Morgan, "Systematic Literature Review of VANET Simulators: Comparative Analysis, Technological Advancements, and Research Challenges," *2024 International Symposium on Parallel Computing and Distributed Systems (PCDS)*, pp. 1-11, 2024, doi: 10.1109/PCDS61776.2024.10743218.

[14] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil and I. H. Hasbullah, "Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey," in *IEEE Access*, vol. 9, pp. 121522-121531, 2021, doi: 10.1109/ACCESS.2021.3109264.

[15] I. M. Varma and N. Kumar, "A comprehensive survey on sdn and blockchain-based secure vehicular networks," *Vehicular Communications*, vol. 44, 2023, doi: 10.1016/j.vehcom.2023.100663.

[16] M. A. Al-Shareeda and S. Manickam, "A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework," in *IEEE Access*, vol. 11, pp. 46218-46228, 2023, doi: 10.1109/ACCESS.2023.3274774.

[17] Z. Ghaleb Al-Mekhlafi *et al*., "Integrating Safety in VANETs: A Taxonomy and Systematic Review of VEINS Models," in *IEEE Access*, vol. 12, pp. 148935-148960, 2024, doi: 10.1109/ACCESS.2024.3476512.

[18] Z. Ghaleb Al-Mekhlafi *et al*., "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575-29602, 2024, doi: 10.1109/JSEN.2024.3436612.

[19] M. Prakash and K. Saranya, "Vanet authentication with privacy-preserving schemes—a survey," in *Proceedings of Fourth International Conference on Communication, Computing and Electronics Systems: ICCCES 2022*, vol. 977, pp. 465–480, 2023, doi: 10.1007/978-981-19-7753-4_36.

[20] S. A. Rashid, L. Audah, M. M. Hamdi, M. S. Abood, and S. Alani, "Reliable and efficient data dissemination scheme in vanet: a review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6423–6434, 2020, doi: 10.11591/ijece.v10i6.pp6423-6434.

[21] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22135026.

[22] A. Bisht and V. Khaitan, "Reliability analysis of 5g-vanet using cloud-fog-edge based architecture," *RAIRO-Operations Research*, vol. 58, no. 1, pp. 129–149, 2024, doi: 10.1051/ro/2023189.

[23] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "Eca-vfog: An efficient certificateless authentication scheme for 5g-assisted vehicular fog computing," *Plos one*, vol. 18, no. 6, 2023, doi: 10.1371/journal.pone.0287291.

[24] Y. Sun, R. Lu, X. Lin, X. Shen and J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589-3603, 2010, doi: 10.1109/TVT.2010.2051468.

[25] P. Sarkar *et al*., *The development and implementation of an intelligent transportation system with 5g capability* CRC Press, 2025.

[26] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for vanet," *Wireless networks*, vol. 19, pp. 1441–1449, 2013, doi: 10.1007/s11276-013-0543-7.

[27] Y. Rajkumar and S. Santhosh Kumar, "A comprehensive survey on communication techniques for the realization of intelligent transportation systems in iot based smart cities," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 1263–1308, 2024, doi: 10.1007/s12083-024-01627-9.

[28] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559–2564, 2014, doi: 10.1016/j.eswa.2013.10.003.

[29] X. Liu, Z. Fang and L. Shi, "Securing Vehicular Ad Hoc Networks," *2007 2nd International Conference on Pervasive Computing and Applications*, pp. 424-429, 2007, doi: 10.1109/ICPCA.2007.4365481.

[30] J. P. Hubaux, S. Capkun and Jun Luo, "The security and privacy of smart vehicles," in *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49-55, 2004, doi: 10.1109/MSP.2004.26.

[31] S. Jiang, X. Chen, Y. Cao, T. Xu, J. He and Y. Cui, "APKI: An Anonymous Authentication Scheme Based on PKI for VANET," *2022 7th International Conference on Computer and Communication Systems (ICCCS)*, pp. 530-536, 2022, doi: 10.1109/ICCCS55155.2022.9845923.

[32] C. Zhang, X. Lin, R. Lu and P. . -H. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," *2008 IEEE International Conference on Communications*, pp. 1451-1457, 2008, doi: 10.1109/ICC.2008.281.

[33] C. Zhang, X. Lin, R. Lu, P. -H. Ho and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368, 2008, doi: 10.1109/TVT.2008.928581.

[34] A. A. Abbood *et al*., "Benchmarking bilinear pair cryptography for resource-constrained platforms using raspberry pi," *WSEASTransactions on Information Science and Applications*, vol. 22, pp. 245–257, 2025, doi: 10.37394/23209.2025.22.21.

[35] A. Sharma and K. Pandey, "Recent advancements in techniques used to solve the rsu deployment problem in vanets: A comprehensive survey," *International Journal of Sensors Wireless Communications and Control*, vol. 12, no. 3, pp. 184–193, 2022, doi: 10.2174/2405520415666220217152355.

[36] S. S. Kanumalli, A. Ch, and P. S. R. C. Murty, "Secure v2v communication in iov using ibe and pki based hybrid approach," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, 2020, doi: 10.14569/IJACSA.2020.0110157.

[37] M. M. Hamdi, Y. A. Yussen and A. S. Mustafa, "Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A

Review," *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-7, 2021, doi: 10.1109/HORA52670.2021.9461327.

[38] M. Al Shareeda, A. Khalil and W. Fahs, "Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm," *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018, doi: 10.1109/ACIT.2018.8672687.

[39] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for vanet," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.

[40] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Specs: Secure and privacy enhancing communications schemes for vanets," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011, doi: 10.1016/j.adhoc.2010.05.005.

[41] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," in *IEEE Access*, vol. 8, pp. 91028-91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[42] Y. Liu, L. Wang and H. -H. Chen, "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks," in *IEEE Transactions on Vehicular Technology,* vol. 64, no. 8, pp. 3697-3710, 2015, doi: 10.1109/TVT.2014.2358633.

[43] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016, doi: 10.1109/JIOT.2016.2579198.

[44] W. Shi and S. Dustdar, "The Promise of Edge Computing," in *Computer*, vol. 49, no. 5, pp. 78-81, 2016, doi: 10.1109/MC.2016.145.

[45] M. N. Tahir, M. Katz and U. Rashid, "Analysis of VANET Wireless Networking Technologies in Realistic Environments," *2021 IEEE Radio and Wireless Symposium (RWS)*, pp. 123-125, 2021, doi: 10.1109/RWS50353.2021.9360381.

[46] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, 2020, doi: 10.1016/j.vehcom.2020.100247.

[47] R. I. Abdelfatah, N. M. Abdal-Ghafour and M. E. Nasr, "Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions," in *IEEE Access*, vol. 10, pp. 1096-1115, 2022, doi: 10.1109/ACCESS.2021.3137877.

[48] S. Son, J. Lee, Y. Park, Y. Park and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 1346-1358, 2022, doi: 10.1109/TNSE.2022.3142287.

[49] V. O. Nyangaresi, A. J. Rodrigues, and N. K. Taha, "Mutual authentication protocol for secure vanet data exchanges," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, vol. 382, pp. 58–76, 2021, doi: 10.1007/978-3-030-78459-1_5.

[50] P. Wang, C. -M. Chen, S. Kumari, M. Shojafar, R. Tafazolli and Y. -N. Liu, "HDMA: Hybrid D2D Message Authentication Scheme for 5G-Enabled VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071-5080, 2021, doi: 10.1109/TITS.2020.3013928.

[51] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar and M. A. Saleem, "Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12158-12167, 2021, doi: 10.1109/TVT.2021.3118892.

[52] Y. Zhou *et al*., "An Efficient Identity Authentication Scheme With Dynamic Anonymity for VANETs," in *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 10052-10065, 2023, doi: 10.1109/JIOT.2023.3236699.

[53] K. Lim, K. M. Tuladhar, X. Wang and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 478-483, 2017, doi: 10.1109/UEMCON.2017.8249091.

[54] J. Zhang, H. Zhong, J. Cui, L. Wei and L. Liu, "CVAR: Distributed and Extensible Cross-Region Vehicle Authentication With Reputation for VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 1, pp. 74-89, 2024, doi: 10.1109/TITS.2023.3306547.

[55] S. Goudarzi *et al*., "A privacy-preserving authentication scheme based on elliptic curve cryptography and using quotient filter in fog-enabled vanet," *Ad Hoc Networks*, vol. 128, 2022, doi: 10.1016/j.adhoc.2022.102782.

[56] H. Tahir, K. Mahmood, M. F. Ayub, M. A. Saleem, J. Ferzund and N. Kumar, "Lightweight and Secure Multi-Factor Authentication Scheme in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 11, pp. 14978-14986, 2023, doi: 10.1109/TVT.2023.3286187.

[57] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, "A novel ddos mitigation strategy in 5g-based vehicular networks using chebyshev polynomials," *Arabian Journal for Science and Engineering*, vol. 49, pp. 11991–12004, 2024, doi: 10.1007/s13369-023-08535-9.

[58] Z. G. Al-Mekhlafi *et al*., "Efficient authentication scheme for 5g-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073543.

[59] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-cppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5g-enabled vehicular system," *Plos one*, vol. 18, no. 10, 2023, doi: 10.1371/journal.pone.0292690.

[60] S. Chen, Y. Liu, J. Ning, and X. Zhu, "Basrac: An efficient batch authentication scheme with rule-based access control for vanets," *Vehicular Communications*, vol. 40, 2023, doi: 10.1016/j.vehcom.2023.100575.

[61] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar and N. Kumar, "A Novel Lightweight Authentication Protocol for Emergency Vehicle Avoidance in VANETs," in *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14248-14257, 2021, doi: 10.1109/JIOT.2021.3068268.

[62] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, "Authentication-based secure data dissemination protocol and framework for 5g-enabled vanet," *Future Internet*, vol. 12, no. 4, 2020, doi: 10.3390/fi12040063.

[63] M. Ouaissa, M. Houmer and M. Ouaissa, "An Enhanced Authentication Protocol based Group for Vehicular Communications over 5G Networks," *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1-8, 2020, doi: 10.1109/CommNet49926.2020.9199641.

[64] S. Soleymani, M. Anisi, A. H. Abdullah, M. A. Ngadi, S. Goudarzi, M. K. Khan, and M. N. Kama, "An authentication and plausibility model for big data analytic under los and nlos conditions in 5g-vanet," *Science China Information Sciences*, vol. 63, no. 220305, 2020, doi: 10.1007/s11432-019-2835-4.

[65] V. O. Nyangaresi, A. J. Rodrigues and S. O. Abeka, "Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications," *2020 16th International Computer Engineering Conference (ICENCO)*, pp. 25-30, 2020, doi: 10.1109/ICENCO49778.2020.9357372.

[66] M. Asghar, R. R. M. Doss and L. Pan, "A Scalable and Efficient PKI Based Authentication Protocol for VANETs," *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1-3, 2018, doi: 10.1109/ATNAC.2018.8615224.

[67] S. Tangade, S. S. Manvi and P. Lorenz, "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647-8655, 2018, doi: 10.1109/TVT.2018.2839979.

[68] Y. Cao, S. Xu, X. Chen, Y. He, and S. Jiang, "A forward-secure and efficient authentication protocol through lattice-based group signature in vanets scenarios," *Computer Networks*, vol. 214, 2022, doi: 10.1016/j.comnet.2022.109149.

[69] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao and Y. He, "An Efficient and Secure Anonymous Authentication Scheme for VANETs Based on the Framework of Group Signatures," in *IEEE Access*, vol. 6, pp. 62584-62600, 2018, doi: 10.1109/ACCESS.2018.2876126

[70] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An efficient distributed key management scheme for group-signature based anonymous authentication

in vanet," *Security and Communication Networks*, vol. 5, no. 1, pp. 79–86, 2012, doi: 10.1002/sec.302.

[71] J. Zhang, J. Cui, H. Zhong, I. Bolodurina and L. Liu, "Intelligent Drone-assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-Hoc Networks," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2982-2994, 2021, doi: 10.1109/TNSE.2020.3029784.

[72] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," *Journal of Information Security and Applications*, vol. 48, 2019, doi: 10.1016/j.jisa.2019.06.010.

[73] H. Khalid *et al*., "HOOPOE: High Performance and Efficient Anonymous Handover Authentication Protocol for Flying Out of Zone UAVs," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10906-10920, 2023, doi: 10.1109/TVT.2023.3262173.

[74] J. Lee, G. Kim, A. K. Das and Y. Park, "Secure and Efficient Honey List-Based Authentication Protocol for Vehicular Ad Hoc Networks," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2412-2425, 2021, doi: 10.1109/TNSE.2021.3093435.

[75] P. Mall, R. Amin, M. S. Obaidat, and K.-F. Hsiao, "Comsec++: Puf-based secured light-weight mutual authentication protocol for drone-enabled wsn," *Computer Networks*, vol. 199, 2021, doi: 10.1016/j.comnet.2021.108476.

[76] S. A. Chaudhry *et al*., "A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2401-2410, 2023, doi: 10.1109/TITS.2021.3134643.

[77] B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in vanet," *Vehicular Communications*, vol. 34, 2022, doi: 10.1016/j.vehcom.2021.100414.

[78] M. Takehiko, H. Okazaki, K. Arai, Y. Futa, and Y. Hiroaki, "Formal security verification for searchable symmetric encryption using proverif," *IEICE Proceedings Series*, vol. 86, 2024, doi: 10.34385/proc.86.We-AM-1-2-3.

[79] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutorial," *Version from*, pp. 5–16, 2018.

[80] V. Cheval, V. Cortier and A. Debant, "Election Verifiability with ProVerif," *2023 IEEE 36th Computer Security Foundations Symposium (CSF)*, pp. 43-58, 2023, doi: 10.1109/CSF57540.2023.00032.

[81] J. Zhang, L. Yang, W. Cao and Q. Wang, "Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif," in *IEEE Access*, vol. 8, pp. 23674-23688, 2020, doi: 10.1109/ACCESS.2020.2969474.

[82] J. Yao, C. Xu, D. Li, S. Lin, and X. Cao, "Formal verification of security protocols: Proverif and extensions," in *Artificial Intelligence and Security*, vol. 13339, pp. 500–512, 2022, doi: 10.1007/978-3-031-06788-4_42.

[83] T. Mieno, H. Okazaki, K. Arai and Y. Futa, "How to Formalize Loop Iterations in Cryptographic Protocols Using ProVerif," in *IEEE Access*, vol. 12, pp. 31605-31625, 2024, doi: 10.1109/ACCESS.2024.3368453.

[84] T. Mieno, H. Okazaki, K. Arai, Y. Futa, and H. Yamamoto, "Formal security verification for searchable symmetric encryption using proverif," in *2024 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 419–424, 20224, doi: 10.34385/proc.86.We-AM-1-2-3.

[85] M. Scott, "Miracl-a multiprecision integer and rational arithmetic c/c++ library," *http://www. shamus. ie*, 2003.