An Efficient Privacy-Preserving Data Aggregation Protocol for Edge Computing Assisted VANETs

Nizamud Din*, Muhammad Sadiq Khan†, Attaullah‡

Abstract

Edge computing empowers Vehicular Ad-hoc Networks (VANETs) to perform local computations on data gathered by vehicles for decision-making. Privacy-preserving data aggregation is essential for reliable decisions and timely responses. This paper proposes a privacy-preserving data aggregation protocol using homomorphic signcryption for edge-enabled VANETs. The proposed protocol provides essential security attributes, including privacy protection, authentication, and data integrity. Additionally, it enables edge nodes to perform operations on encrypted data. A comparative analysis with state-of-the-art existing schemes is presented. The analysis shows that the proposed scheme reduces computation cost from 72% to 98% at the vehicular, edge and cloud servers and 54% to 75% communication overhead in the registration phase. In the data upload request phase, the proposed scheme reduces computation cost from 72% to 98% at vehicular, edge and cloud servers and communication overhead from 16% to 36%. While in the encrypted data generation/aggregation/decryption phase, the proposed protocol reduces computation cost from 25% to 97% at vehicular, edge and cloud servers and communication overhead from 6% to 89%. The proposed scheme exhibits lower implementation and memory consumption, making it an attractive solution for resource-constrained environments.

Keywords: Confidentiality, Privacy, Signcryption, Data Aggregation, Edge Computing, Vehicular Ad-hoc Networks.

Introduction

Vehicular Ad-hoc Networks (VANETs) (Al-Sultan et al., 2014) are becoming a key enabler technology of the intelligent transportation system (Shan et al., 2021). It performs vehicle-to-vehicle and infrastructure communication, where vehicles share information with infrastructure e.g. roadside units (RSUs) (Lien et al., 2019; Masmoudi et al., 2019). The VANETs provide high-level traffic management that can improve the safety and traffic efficiency of vehicles. However, the open internet is a big challenge and may be vulnerable to various attacks on privacy, communication, and identity tracking. Moreover, it requires more

*Corresponding Author: Department of Computer Science, University of Chitral, Chitral 17200, Pakistan, nizam@uoch.edu.pk

† Department of Computer Science, University of Chitral, Chitral 17200, Pakistan, sadiq.khan@uoch.edu.pk

‡ Department of Computer Science, University of Chitral, Chitral 17200, Pakistan, atta.ullah@uoch.edu.pk

bandwidth and face numerous other challenges such as quick response time, communication and computation overheads. One of the solutions to these challenges is mobile cloud computing (MCC) (Rahimi et al., 2014) with integrated computation and communication technologies. The MCC allows users to run their application services on the cloud, enabling an extensive analysis of data, solving storage issues and reducing energy consumption. Bitam et al. (2015) propose a cloud service model for the VANET applications to enhance the quality of service (QoS) by utilizing cloud resources for computation purposes. However, sending a large amount of data in raw form to the cloud for processing and analysis again raises an issue of the utilization of unnecessary bandwidth and also faces a high latency.

Data Aggregation (DA) is an efficient approach that merges the related information and removes the redundancy. A privacy-preserving scheme is proposed for securing smart grid communication with reduced authentication costs using function encryption (Yu et al., 2025). It also secures the smart grid from false data injections and modification attacks. Further, a multi-dimensional DA privacy-preserving scheme is proposed with data verification and authentication for the smart grid named fog-enabled smart grid (Tan et al., 2014; Liu et al., 2019). Pan et al. (2019) extend the privacy-preserving schemes and present a scheme based on bilinear pairing and Paillier cryptosystem on edge-enabled VANETS, performs batch operation on aggregated data, ensures source authentication and privacy of terminals.

This work proposes privacy-preserving DA protocols using a homomorphic signcryption approach on Edge-enabled VANETs. The proposed protocol enables edge nodes to perform aggregation on signcrypted data. It provides essential security attributes, reduced implementation costs, and computation and communication overheads.

The main contributions of the present research are as follows:

Proposes privacy-preserving data aggregation scheme using a homomorphic signcryption approach on Edge-enabled VANETs. The proposed scheme provides integrity, authenticity and confidentiality of generated and aggregated data for smart communication. The scheme also reduces implementation, computation cost and communication overhead.

The rest of the paper is organized as follows: Section 2 presents related work. Section 3 presents preliminaries. Section 4 describes the proposed scheme, Section 5 presents an analysis, and Section 6 concludes the paper.

Related Work

Currently, few state-of-the-art approaches are focusing on the security and privacy preservation of relevant applications of smart grids

and VANETs. The security of smart grid applications is a key requirement to preserve the privacy of a residential community and required security approaches to achieve the integrity, authentication, and confidentiality of the collected information simultaneously. Such approaches should be efficient in communication, computation, and response time with reduced overhead. Lu et al. (2012) present an efficient aggregation scheme based on homomorphic encryption (HE). This scheme enables a privacy-preserving DA scheme on the gateway and secures the information of smart grid users.

Rafik et al. (2017) propose a multi-recipient encryption scheme (MRES) for the security of multidimensional data. The authors have used the elliptic curve El-Gamal (ECEG) encryption and digital signature with batch verification for nodes to achieve data integrity and authentication. Zhang et al. (2018) propose a scheme based on the PHE in fog computing. Their scheme realizes the privacy protection, non-repudiation, and unforgeability of hybrid IoT devices and improved the efficiency of control centers and fog nodes with reduced communication overheads. Ming et al. (2019) present a privacy-preserving data aggregation and authentication scheme in a smart grid scenario. The authors have implemented the Paillier cryptosystem using HE algorithm with a few other assumptions. During the data transmission, they achieved data integrity and authentication with resistance to various attacks, e.g., injection, modification, replay and forgery. However, one-dimensional DA techniques do not provide a fine-grained security solution. Zhao et al. (2022) present a privacy-preserving multi-dimensional DA scheme in a smart grid with HE. The study has proved the security of the scheme in random oracle model for fulfilling the security and privacy measures with reduced computation and communication overheads.

VANETs also have bandwidth and privacy issues for the uploaded data, and DA is an efficient solution to resolve this issue. Rafik et al. (2020) present a privacy-preserving DA scheme for edge-enabled computation of VANETs, using a bilinear pairing and Paillier HE. The scheme preserves data privacy and integrity and source authentication. Zuo et al. (2020 present an efficient and secure multidimensional DA scheme called ESMA for smart grids. This multidimensional DA expands the application of privacy in smart grids and fulfils the demands of the fine-grained analysis of multidimensional data. Guan et al. (2019) proposed a privacy-preserving MDA scheme without a trusted authority in the smart grid.

Preliminaries

This Section provides a brief introduction of the security notions used in the proposed scheme:

Definition: Elliptic Curve: Let F_n denote a finite field of prime order $n \geq 2^{160}$. An elliptic curve E over F_n is defined by an equation $y^2 = x^3 + ax + b$ also satisfy $4a^3 + 27b^2 \neq 0$ where $a, b \in F_n$. The points (x, y) on the E from an additive Abelian group denoted by $E(F_n)$

Definition: Bilinear maps: Let an additive group $E(F_n)$ having generator G and a multiplicative group F_n having generator g, both of prime order n. A bilinear map $e : G \times G \rightarrow g$ has properties:

- Bilinearity: $\forall P, G \ E(F_n)$ and $\forall a, b \in F_n.; \ e(aP ; bQ) = e(P, Q)^{ab}$.
- Non-degeneracy: $e(P, Q) \neq 1$.
- Computability: $\forall P, G \ E(F_n)$ There exists an efficient algorithm to compute $e(P, Q)$ in polynomial time.

Definition: Elliptic Curve Discrete Logarithm Problem (ECDLP): Let E be an elliptic curve defined over F_n . Let two given points $P \ and \ Q \in E(F_n)$ such that $P = d\ Q$ Computing d from P and Q is ECDLP.

Methodology

This section presents the detailed methodology of how the proposed scheme works. The proposed scheme consists of seven phases: System Initialization, Key Generation, Registration, Data Upload Request, Encrypted Data Generation, Encrypted Data Aggregation and Data Decryption.

System Model

The proposed scheme system model consists of entities: Vehicular Data Sensor (VDS), Vehicular Server (VS), Edge Server (ES), and the Cloud Server (CS) as shown in Figure 1.

Vehicular Data Sensor (VDS)

Data sensors installed on vehicles that collect data and send it to the Vehicular Server.

Vehicular Server (VS)

A server on the vehicle, such as an onboard unit. VS collects the data from vehicle sensors and encrypts and sends it to the nearest Edge Server.

Edge Server (ES)

Roadside units, collect data from the VSs in their locality, verifies, aggregates and forwards it to the Cloud Server.

Cloud Server (CS)

High computational resources, collects aggregated data from all nearby ESs, decrypts aggregated data, analyze and takes decisions to facilitate vehicles and pedestrians.

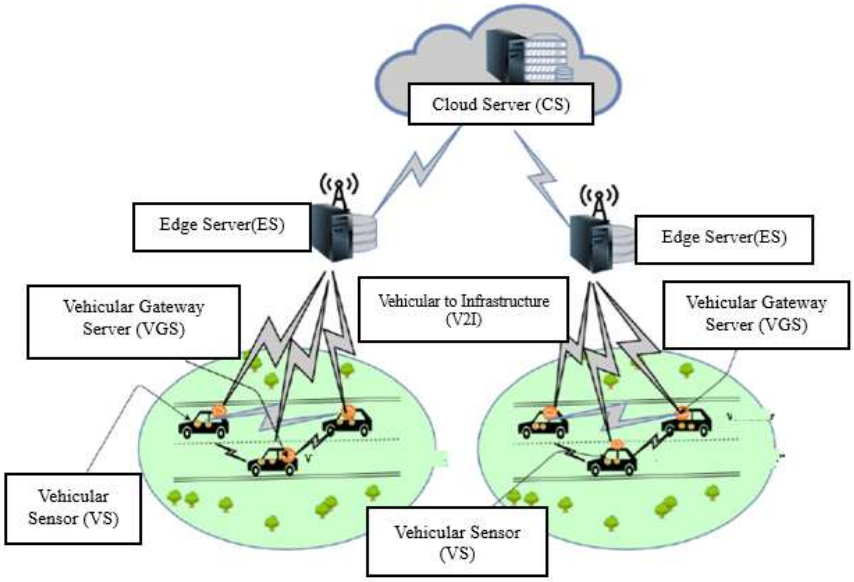

Figure 1: Illustration of the system model.

System Initialization

In this phase, the system is initialized by the CS. It selects a finite multiplicative field F_n and an additive group of elliptic curves $E(F_n)$ both of order n, a hash functions $H_1 : \{0,1\}^* \rightarrow \{0,1\}^*$ and publish public parameters params: $(F_n, E(F_n, G, H_1)$ to the entire system.

Key Generation

CS select $CS_{pr} \in F_n$ as the private key and computes their public key $CS_{pu} = CS_{pr}.G$ and publish to the entire system. The ES_i having identity ID_{ES_i} select ES_{pri} as the private key, computes and publish public key $ES_{pu} = ES_{pri}G$.

The VS_i having identity ID_{vsi}, select $VS_{pri} \in Z_n$ as the private key, computes and publishes the public key $VS_{pui} = VS_{pri}G$.

Registration

In this phase, each VS and ES register themselves with CS, the registration is elaborated as follows.

ES Registration

The ES_i having identity ID_{ESi}, private and public keys ES_{pui}. The ES_i, choose and signcrypt their credential Identity ID_{ES_i}, public key ES_{pui}, session key S_{ki}. and timestamp T_{reg} using forward secure signcryption as:

- Select $r \in F_n$
- Computes $R = r.G$
- Computes $K_1. = H_1(r.CC_{pu})$
- Computes $x = H_1(ID_{ESi} \,||\, ES_{pui}||S_{k1}||T_{reg})$
- Computes $C = Enc_{K1}(ID_{ESi} \,||\, ES_{pui}||S_{k1}||T_{reg})$
- Computes $S = \frac{r+ES_{pri}}{x}$
- Send forward secure, signcrypted text $\varphi = (R, C, S)$ to CS as request registration through the public channel.

On receiving the registration request, CS unsigncrypt received information as:

- Select $K_1 = H_1(CC_{pr}.R)$
- Computes $ID_{ESi} \,||ES_{pui}||S_{k1}||T_{reg} = Dec_{k1}(C)$
- Computes $x = H_1(ID_{ESi} \,||\, ES_{pui}||S_{k1}||T_{reg})$
- If $R + ES_{pui} = \frac{S.G}{x}$ else $\perp$
- CS regenerate timestamp T_{regcc}
- Encrypt $C = Enc_{cs_{ki}}(ES_{pui}||S_{k1}||T_{reg})$
- Send to C to ES_i

On receiving C, ES_i decrypt received information as:

- Computes $ES_{pui}||S_{k1}||T_{reg} = Dec_{cs_{ki}}(C)$
- if received ES_{pui}, S_{ki} is equal to stored ES_{pui}, S_{ki}
- Registration Complete

VS Registration

The VS_i having identity ID_{VSi}, private and public key VS_{pui}. The VSi Choose and signcrypt their credential Identity ID_{VSi}, public key VS_{pui}, session key S_{k1}. and timestamp T_{reg} using forward secure signcryption as:

- Select $r \in F_n$
- Computes $R = r.G$
- Computes $K_1. = H_1(r.CC_{pu})$
- Computes $x = H_1(ID_{VSi} \,||\, VS_{pui}||S_{k1}||T_{reg})$
- Computes $C = Enc_{K1}(ID_{VSi} \,||\, VS_{pui}||S_{k1}||T_{reg})$
- Computes $S = \frac{r+VS_{pri}}{x}$
- Send forward secure signcrypted text $\varphi = (R, C, S)$ to CS as requested, registration through the public channel.

On receiving the registration request CS Unsigncrypt received information as:

- Select $K_1 = H_1(CC_{pr}.R)$
- Computes $ID_{VSi} \,||VS_{pui}||S_{k1}||T_{reg} = Dec_{k1}(C)$
- Computes $x = H_1(ID_{VSi} \,||\, VS_{pui}||S_{k1}||T_{reg})$
- If $R + VS_{pui} = \frac{S.G}{x}$ else $\perp$
- CS regenerate timestamp T_{regcc}
- Encrypt $C = Enc_{cs_{ki}}(VS_{pui}||S_{k1}||T_{reg})$
- Send to C to VS_i

On receiving C, VS_i decrypt received information as:

• Computes $VS_{pui}||S_{k1}||T_{reg} = Dec_{cs_{ki}}(C)$
• if received VS_{pui}, S_{ki} is equal to stored VS_{pui}, S_{ki}
• Registration Complete

Data Upload Request

For efficient road service utilization, CC needs to collect the data from VS periodically, broadcasts data collection request to selected ES, which rebroadcasts the request to all nearby VS.

CS generates a request for information $m_i : VS_i i \rightarrow CS$

- Select $v \in F_n$
- Computes $r = H_1(r.G||m_i)$
- Computes $s = \frac{v}{r+CS_{pri}} \, mod \, n$
- CC: Send signed text $\varphi = (m_i, r, s)$ to ES_i

• Computes $K_1 = H_1\big(s.(CS_{pui} + rG)\big)$
• Computes $r = H_1(s.(||m_i))$
• Accept the request information if $r' = r \, else \perp$

$ES_i \rightarrow CS_i$

• Select $v \in F_n$
• Computes $r = H_1(r.G||m_i)$
Computes $s = \frac{v}{r+CS_{pri}} \ mod \ n$
Send signed text $\varphi = m_i, r, s)$ to ES_i

ES_i

• Computes $K_1 = H_1\left(s.\left(CS_{pui} + r.G\right)\right)$
• Computes $r' = H_1(K_1||m_i)$
• Accept the request information if $r' = r$ else $\perp$.

Encrypted Data Generation

In this phase, VS_i belong to the same ES_i first, signcrypt the collected data using $HSign$ on ECC as:

• Select $r \in Z_q$
• Computes $c_0 = r.G$ and $c_1 = P_{mi} + r.CS_{pu}$
• Computes $c_2 = \left(VS_{pri} + r\right).ES_{pui} + c_1$.
• Send homomorphic signcrypted text $C = c_0, c_1, c_2 \ to \ E \ Si$

Encrypted Data Aggregation

Receiving the ciphertext VS_{pui}, c_0, c_1, c_2 from the ES_iVerify the ciphertext as:

• Aggregate all VS_ipublic key $AVS_{pui} = \sum_{i=1}^{n} S_{pki}$
• Aggregate Homomorphic Signcrypted texts
  - Computes $C_0 = \sum_{i=1}^{n} c_{0i}$
  - Computes $C_1 = \sum_{i=1}^{n} c_{1i}$
  - Computes $C_2 = \sum_{i=1}^{n} c_{2i}$
• Forward $AVS_{pui}, C_0, C_1, C_2 \ to \ CC$

Data Decryption

When messages are aggregated and received AVS_{pui}, C_0, C_1, C_2 . from the ES_i , CS first verify as:

• $\mu = CC_{pr}\left(VS_{pk}\right) + C_0) + C_1$
• Accept if $\mu = C_2$. else $\perp$ and exit
• Decrypt $\sum_{i=1}^{n} P_{mi} = (C_1 - CC_{pr}C_0)$
• Messages aggregated $\sum_{i=1}^{n} P_{mi}$

Results and Discussions

This section presents detailed correctness, security and performance analysis of the proposed scheme. The comparative analysis with state-of-the-art existing schemes is presented as well.

Correctness Analysis

The correctness analysis is based on Theorems 1 and 2, respectively.

Theorem 1

The homomorphic signcryption/unsigncryption is correct if $C_1 - CC_{pr}C_0 = \sum_{i=1}^{n} m_i$ holds so the homomorphic signcryption/unsigncryption is correct.

Proof 1:

Let $C_1 - CC_{pr}C_0$

$$= \sum_{i=1}^{n} c_{i1} - CC_{pr}C_0 = \sum_{i=1}^{n} c_{i1} - CC_{pr}\sum_{i=1}^{n} c_{i0}$$

$$= \sum_{i=1}^{n}(P_{mi} + r.CC_{pu}) - CC_{pr}\sum_{i=1}^{n} r_i\, G$$

$$= \sum_{i=1}^{n} P_{mi} + \sum_{i=1}^{n} r_i\ CC_{pu}) - CC_{pr}\sum_{i=1}^{n} r_i\, G$$

$$= \sum_{i=1}^{n} P_{mi} + \sum_{i=1}^{n} r_i\ CC_{pr}G) - CC_{pr}\sum_{i=1}^{n} r_i\, G = \sum_{i=1}^{n} P_{mi} = \sum_{i=1}^{n} m_i$$

The homomorphic signcryption/unsigncryption is correct if $C_1 - CC_{pr}C_0 = \sum_{i=1}^{n} m_i$ holds so the homomorphic signcryption/unsigncryption is correct.

Theorem 2

The homomorphic unsigncryption verification is correct if $\sum_{i=1}^{n} C_{i2} = AVS_{pui}CC_{pr} + C_0 + C_1$.

Proof 2:

Let

$$AVS_{pui}CC_{pr} + C_0 + C_1 = \sum_{i=1}^{n} AVS_{pui}CC_{pr} + \sum_{i=1}^{n} P_{mi} + CC_{pr}C_0$$

$$= \sum_{i=1}^{n} AVS_{pui}CC_{pr} + \sum_{i=1}^{n} P_{mi} + CC_{pr}\ \sum_{i=1}^{n} r_i\, G$$

$$= \sum_{i=1}^{n} AVS_{pri}CC_{pu} + \sum_{i=1}^{n} P_{mi} + \sum_{i=1}^{n} r_i CC_{pu}$$

$$= \sum_{i=1}^{n}(AVS_{pri} + r_i)CC_{pu} + \sum_{i=1}^{n} P_{mi} = \sum_{i=1}^{n} C_{i2}$$

The homomorphic unsigncryption verification is correct as $C_1 - CC_{pr}C_0 = \sum_{i=1}^{n} m_i$ holds.

Security Analysis

This section presents a detailed security analysis of proposed. A detailed comparative security analysis with existing schemes is also presented in Table 1.

Privacy

In the proposed scheme, the VS_i computes the homomorphic signcrypted text $C = c_0, c_1, c_2$ to ES_i using elliptic curve homomorphic signcryption that is IND-CPA secure and send to the VS_i and without knowing the secret key the ciphertext can not be obtained. ES_i first aggregates the received messages from the VS_i in communication range and sends the aggregated signcrypted text $AVS_{pui}, C = c_0, c_1, c_2$ to CS, that only can Unsigncrypt the aggregated data not individual data and the privacy of VS_i is protected.

Integrity

In VS_i and ES_i registration phase, use signcryption with forward secrecy that use standard hash function to ensure integrity of registration request messages. In data upload request broadcast standard digital signature is used to ensure integrity of upload request messages. In homomorphic data encryption phase homomorphic signcryption is used to ensure integrity of messages.

Authenticity

Authenticity of data during registration and data upload request. In VS_i and ES_i registration phase uses signcryption with forward secrecy that uses a standard hash function to ensure the authenticity of registration request messages. In data upload request broadcast standard digital signature is used that ensure the authenticity of upload request messages. In the homomorphic data encryption phase, homomorphic signcryption is used that ensures the authenticity of messages.

Table 1: Security comparison of proposed and existing schemes.

Schemes	Conf	Int	Auth	Reg	Smart	VANET
Lu et al. (2012	Yes	Yes	Yes	No	Yes	No
Rafik et al. (2017)	Yes	Yes	Yes	Yes	Yes	No
Zhang et al. (2018)	Yes	Yes	Yes	Yes	Yes	No
Ming et al. (2019)	Yes	Yes	Yes	Yes	Yes	No
Zhao et al. (2022)	Yes	Yes	Yes	Yes	No	Yes
Rafik et al. (2020)	Yes	Yes	Yes	No	Yes	No
Zuo et al. (2020)	Yes	Yes	Yes	Yes	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes	Yes

Performance Analysis

This section provides a comparison of the computational cost and communication overhead of the proposed scheme with state-of-the-art existing schemes. The computational cost depends on the most expensive operations: ECPM, Mexp and BP involve in privacy preserving data communication protocol.

Registration Performance Comparison

In the registration phase, the VS and ES registration performance and percent reduction in performance of the proposed scheme are compared with the state-of-the-art existing schemes as shown in Tables 2, 3 & 4.

Table 2: Registration phase performance comparison of proposed and existing schemes.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Rafik et al. (2017)	1Mexp	1Mexp	I*(Mexp)	i*(|ID + 3n + 2q|)
Zhang et al. (2018)	1ECPM	1ECPM	i*(2ECPM)	i*(|ID + 3n + 2q|)
Ming et al. (2019)	1ECPM	i*(1ECPM)	i*(2ECPM)	i*(|ID + q + 2n|)
Zhao et al. (2022)	1ECPM + 2BP	1ECPM + 2BP	i*(1ECPM + BP)	i*2(|ID+Tre +4n+H|)
Zuo et al. (2020)	1Mexp + 2BP	1Mexp + 2BP	i* (2BP+1Mexp)	i* (|ID + T + 2q|)
Proposed	2ECPM	2ECPM	i*(2ECPM)	i*(2|c+n|)

The percent computation time consumed by these operations on a computer with Intel Core i5-2430 2.4-GHz CPU and 2-GB RAM using cryptographic libraries, MIRACL (github.com, 2020), and PB (Lynn, 2020) is given as modular exponentiation in Mexp = 2.88ms, Bilinear pairing BP = 22.8ms, EC point multiplication ECPM = 0.44ms. The communication overhead (Comm. Overhead) is based on NIST standard parameters size for Paillier encryption 1024-bits and for pairing and ECC a base field size of 160 bits.

Table 3: Registration phase comparison of proposed and existing schemes in milliseconds and bits.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Rafik et al. (2017)	2.88 ms	2.88 ms	2.88 ms	2592 bits
Zhang et al. (2018)	0.4 ms	0.4 ms	0.8 ms	2592 bits
Ming et al. (2019)	0.4 ms	0.4 ms	0.8 ms	1408 bits
Zhao et al. (2022)	46.08 ms	46.08 ms	46.08 ms	928 bits
Zuo et al. (2020)	48.56 ms	48.56 ms	48.56 ms	2176 bits
Proposed	0.8 ms	0.8 ms	0.8 ms	640 bits

Table 4: Registration phase comparison of proposed and existing schemes % cost reduction.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Rafik et al. (2017)	72%	72%	72%	75%
Zhang et al. (2018)	-1%	-1%	0%	75%
Ming et al. (2019)	-1%	-1%	0%	54%
Zhao et al. (2022)	98%	98%	98%	31%
Zuo et al. (2020)	98%	98%	98%	70%

Data Upload Request Performance Comparison

In the data upload request phase, data upload request performance of the proposed scheme is compared with state-of-the-art existing schemes as shown in Tables 5,6 & 7.

Table 5: Data upload request phase performance comparison of proposed and existing schemes.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Zhang et al. (2018)	2BP	i*(ECPM+2BP)	i*(ECPM)	i*(|2ID +2T+2n|)
Zhao et al. (2022)	2BP	i*(ECPM+2BP)	i*(1CPM + BP)	i*2(|ID+Tre+n|)
Proposed	2ECPM	i*2ECPM	i*(2ECPM)	i*(|c+2n|)

Table 6: Data upload request phase performance comparison of proposed and existing schemes in ms and bits.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Zhang et al. (2018)	45.68 ms	46.08 ms	0.4 ms	576 bits
Zhao et al. (2022)	45.68 ms	46.08 ms	0.4 ms	352 bits
Proposed	0.8 ms	0.8 ms	0.8 ms	480 bits

Table 7: Data Upload Request Phase Performance Comparison of Proposed and Existing Schemes % Cost Reduction.

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Zhang et al. (2018)	98%	98%	-1%	16%
Zhao et al. (2022)	98%	98%	-1%	36%

Encrypted Data Generation/Aggregation/Decryption Performance Comparison

In the Data Generation/Aggregation/Decryption phase, the proposed scheme has less computation cost for one device; the same computation advantage can be obtained for more devices. The data upload request performance of the proposed scheme is compared with the existing schemes in Tables 8, 9 & 10.

Table 8: Data generation/aggregation/decryption phase performance comparison of proposed and existing schemes

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Lu et al. (2012)	I*(2Mexp+ECPM)	I*(ECPM+2BP)	I*(Mexp+2BP)	I*|c+2ID+T+n|
Rafik et al. (2017)	I*4ECPM	I*3ECPM	I*3ECPM	I*|c+2ID+T+n|
Zhang et al. (2018)	I*(2(Mexp+2BP)+ECPM^o	I*(2Mexp+4BP)	I*(2Mexp+4BP)	I*|c+2ID+T+n|
Ming et al. (2019)	I*(4ECPM)	I*(4ECPM)	I*(4ECPM)	I*|c+2ID+T+2n|
Zhao et al. (2022)	I*(2Mexp+ECPM)	I*(ECPM+4BP)	I*(2Mexp+2BP)	I*|c+2ID+T+n|
Rafik et al. (2020)	I*(2Mexp+ECPM)	I*(ECPM+2BP)	I*(Mexp+2BP)	I*|c+ID+T+3n|
Zuo et al. (2020)	I*4Mexp	I*(Mexp+2BP)	I*(2Mexp+4BP)	I*|c+ID+T+3q|
Proposed	I*3ECPM	I*2ECPM	I*3ECPM	I*|c+2n|

Table 9: Data generation/aggregation/decryption phase performance comparison of proposed and existing schemes in ms & bits

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Lu et al. (2012)	6.16 ms	46.08 ms	48.56 ms	512 bits
Rafik et al. (2017)	1.6 ms	1.2 ms	1.2 ms	448 bits
Zhang et al. (2018)	51.95 ms	97.12 ms	97.12 ms	736 bits
Ming et al. (2019)	1.6 ms	1.6 ms	1.6 ms	1568 bits
Zhao et al. (2022)	6.16 ms	91.76 ms	97.12 ms	448 bits
Rafik et al. (2020)	6.16ms	46.08 ms	48.56 ms	448 bits
Zuo et al. (2020)	11.52 ms	46.08 ms	97.12 ms	4224 bits
Proposed	1.2 ms	0.8 ms	1.2 ms	480 bits

Table 10: Data generation/aggregation/decryption phase performance comparison of proposed and existing schemes % cost reduction

Schemes	Comp. Cost VS	Comp. Cost ES	Comp. Cost CS	Comm. Overhead
Lu et al. (2012)	80%	98%	97%	6%
Rafik et al. (2017)	25%	33%	9%	-7%
Zhang et al. (2018)	97%	99%	98%	34%
Ming et al. (2019)	25%	5%	25%	69%
Zhao et al. (2022)	80%	99%	98%	-7%
Rafik et al. (2020)	80%	98%	97%	-7%
Zuo et al. (2020)	89%	98%	98%	89%

Conclusions

This paper proposes privacy-preserving data aggregation protocol for edge-assisted Vehicular Ad-hoc Networks (VANETs) using homomorphic signcryption based on Elliptic Curve Cryptography (ECC). The proposed protocol enables edge nodes to operate on encrypted data. It provides essential security attributes, including privacy protection, authentication, and data integrity. A comparative analysis of the proposed scheme with state-of-the-art existing schemes is presented. The analysis shows that the proposed scheme reduces computation cost from 72% to 98% at the vehicular, edge and cloud servers and 54% to 75% communication overhead in the registration phase. In the data upload request phase, the proposed scheme reduces computation cost from 72% to 98% at vehicular, edge and cloud servers and communication overhead from 16% to 36%. In the encrypted data generation /aggregation /decryption phase, the proposed protocol reduces computation cost from 25% to 97% at vehicular, edge and cloud servers and communication overhead from 6% to 89%. Due to its computational and communication efficiency, the proposed scheme is particularly attractive for emerging VANETs.

References

Al-Sultan, S., M. Al-Doori, M., & H. Al-Bayat, A. (2014). A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications, 37, 380-392.

Bitam, S., Mellouk, A., & Zeadally, S. (2015). VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks. IEEE Wireless Communications, 22(1), 96-102.

Guan, Z., Zhang, Y., Zhu, L., & Wu, L. (2019). EFFECT: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. Science China Information Sciences, 62, 32103.

Lien, S.-Y., Hung, S.-C., Deng, D.-J., Lai, C.-L., Lai, C.-L., & Tsai, H.-L. (2019). Low Latency Radio Access in 3GPP Local Area Data Networks for V2X: Stochastic Optimization and Learning. IEEE Internet of Things Journal, 6(3), 4867-4879.

Liu, J.-N., Weng, J., Yang, A., Chen, Y., & Lin, X. (2019). Enabling Efficient and Privacy-Preserving Aggregation Communication and Function Query for Fog Computing-Based Smart Grid. IEEE Transactions on Smart Grid, 11(1).

Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Transaction on Parallel Distributed System, 23(9), 1621-1631.

Masmoudi, A., Mnif, K., & Zarai, F. (2019). A survey on radio resource allocation for V2X communication. Wireless Communications and Mobile Computing (1).

Ming, Y., Zhang, X., & Shen, X. (2019). Efficient privacy-preserving multidimensional data aggregation scheme in smart grid. IEEE Access, 7, 32907–32921.

Pan, J., Cui, J., Wei, L., Xu, Y., & Zhong, H. (169-2019). Privacy-preserving data aggregation scheme for edge computing supported vehicular ad hoc networks. EURASIP Journal on Wireless Communications and Networking.

Rafik, O., Senouci, S., & Feham, M. (2017). Elliptic curve-based secure multidimensional aggregation for smart grid communications. IEEE Sensors Journal, 17(23), 7750–7757.

Rafik, O., & Mohammed Senouci, S. (2020). An Efficient and Secure Multidimensional Data Aggregation for Fog Computing-based Smart Grid. IEEE Internet of Things Journal, 8(8), 6143-6153.

Rahimi, M., Ren, J., Liu, C., Vasilakos, A., & Venkatasubramanian, N. (2014). Mobile Cloud Computing: A Survey, State of Art and

Future Directions. Mobile Networks and Applications, 19, 133–143.

Shan, A., Fan, X., Wu, C., & Zhang, X. (2021). Quantitative Study on Impact of Static/Dynamic Selfishness on Network Performance in VANETs. IEEE Access, 9, 13186-13197.

Tan, Z., Cao, F., Liu, X., Jiao, J., You, W., & Lin, J. (2025). LPPMM-DA: Lightweight Privacy-Preserving Multi-Dimensional and Multi-Subset Data Aggregation for Smart Grid. IEEE Transactions on Smart Grid, 16(2), 1801-1816.

Yu, P., Huang, W., Zhang, R., Qian, X., Li, H., & Chen, H. (2025). GuardGrid: A Queriable and Privacy-Preserving Aggregation Scheme for Smart Grid via Function Encryption. IEEE Internet of Things Journal.

Zhang, Y., Zhao, J., Zheng, D., De, K., Ren, F., Zheng, X., & Shu, J. (2018). Privacy-preserving data aggregation against false data injection attacks in fog computing. Sensors, 18(8), 2659.

Zhao, O., Liu, X., Li, X., Singh, P., & Wu, F. (2022). Privacy-preserving data aggregation scheme for edge computing supported vehicular ad hoc networks. Transactions on Emerging Telecommunications Technologies, 33(5).

Zuo, X., Li, L., Peng, H., Luo, S., & Yang, Y. (2020). Privacy-Preserving Multidimensional Data Aggregation Scheme Without Trusted Authority in Smart Grid. IEEE Systems Journal, 15(1), 395-406.

github.com. (2020). Retrieved 2024, from https://github.com/miracl/MIRACL

Lynn, B. (2020). PBC Library. Retrieved from http://crypto.stanford.edu/pbc/; pbc-0.5.14