International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Data Sharing Scheme for Vehicular Cloud Networks Using an Optimized RSA Algorithm

Varalakshmi J*[1],S.Dhanasekaran[2]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract : In modern years, vehicular cloud computing (VCC) has come up with innovative technology to give continuous information to the vehicles from every time and everywhere. VCC delivers both secure and non-secure information to its users. The vehicles carry low computational powers, storage, etc., so they gather and forward their information to the vehicular cloud for computing and storage. Nevertheless, privacy and security are the primary concerns we must focus on every VCC system. This study proposes secure and effective data-sharing scheme for vehicular cloud computing environments using an optimized RSA algorithm that encrypts the data initially and stores it in the cloud to protect it from unauthorized access. The method performs key generation process optimally using the Spiral learning centred Coati Optimization Algorithm (SLCOA) which helps to improve the system's security further. The simulation outcomes proved that our model is secure and well suitable for VCC compared to other related schemes.

Keywords*: Vehicular cloud computing, Secure Data Transmission, Encryption, Decryption, and Rivest Shamir Adelman*

1. INTRODUCTION

In recent times, vehicles have not been connected only to the Internet via wireless communication and also become network nodes that can carry out different applications in real-time [1]. Mainly, some applications like big data analysis and image processing using machine learning need high computing power. To run these kinds of applications smoothly, VCC is the best solution [2]. In VCC, drivers can collaborate with each other for sharing the information as well as rent different unused vehicle resources like network storage, network connectivity and computing power. The architecture of VCC is shown in fig.1 [3].

Therefore, the vehicular device relates to other amenities such as roadside units, vehicles, and traditional clouds. Hence, VCC suffers from several security threads like brute force attacks and Distributed Denial Service (DDoS) specifically aimed at disrupting the functioning and performance of services [3, 4]. In current years,many security researchers have been working inflexibly for ensuring the privacy and security of the data. Still, the current privacy preservation models reach many disadvantages such as incorrect data analysis, less data privacy, and complete rely on third parties [5]. Hence, data privacy is an additional important disquiet from the perspective of vehicular cloud data [6].

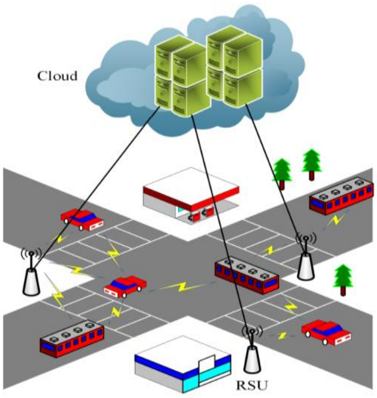


Figure 1: Architecture of VCC [3]

To achieve privacy, Encryption and Decryption are most the widely used methods, and there exist various methods of execution. The two algorithms of encryption and decryption are symmetric and asymmetric based cryptographic algorithms [7]. Some of the well-known asymmetric encryption in use are Elliptic curve cryptography (ECC), ElGmal encryption, Rivest Shamir Adelman, etc. Likely, some of the symmetric models in use Blowfish, Advanced encryption standard (AES), etc. The main difference between these methods is symmetric model utilizes a single key for both encoding and decoding. On the further side, asymmetric model uses two separate keys say public and private keys for data encryption and decryption. Symmetric encryption is lightly less modern compared to Asymmetric

[1] *Saveetha Engineering College, Thandalam, Chennai, India,602 105.*
0000-0002-4451-9408
[2]*Kalasalingam Academy of Rearch and Education, Krishnankovil, Tamilnadu, India, 626126*
0000-0002-5409-2057
Email ID: [1]vara.mail2@gmail.com*
Email ID: [2]srividhans@gmail.com

encryption [8, 9]. RSA is still the mainly employed and used cryptosystem, other than it has some.

Difficulty with random key generation, which also affects the system's performance. The developed RSA algorithm mainly works as a key for providing secure communication in the vehicular cloud etwork. The major contributions of the paper are enlisted as follows;

- The system develops ORSA approach to encrypt the vehicular cloud data that helps to provide secure data communication in the network and avoids third party attacks.
- The system uses SLCOA model for optimum key generation in RSA, which further increases the security of the network and the local optimal issue of the optimization model is solved using spiral learning strategy.

The remainder of the manuscript is organized as follows: the survey of existing models was presented in Section 2. The working process of proposed methodology is presented in Section 3. In Section 4 and 5 the performance analysis and the conclusions with future discussions are discussed.

2.LITERATURE SURVEY

This section surveys the recent security approaches to protect the vehicular cloud data.

A lightweight cryptographic approach for connected vehicles on edge devices was suggested by **Shabi Boubaker *et al.* [10]** which also encrypts exchanged data; the system used a light encryption device (LED) block cipher. he results showed that the system taken 8.728ns and 8.332ns time to encrypt and decrypt the data. A frameworks of data privacy preservation and location obfuscation in cloud networks was suggested by **Hani Al-Balasmeh *et al.* [11].** The system comprised five stages: registration, data privacy block' processing, obfuscation data' segregation, authentication, and offering cryptographic security. The encryption was performed using RSA algorithm and the system taken around maximum 2500000s time for encryption and decryption. For cloud-assisted vehicular networks, **Zhiquan Liu *et al.* [12]** proffered a privacy-preserving reputation updating (PPRU) scheme to encrypt the data for safe transmission. The system used ECC and the paillier algorithm in the network. The findings showed that the computation and communication cost of the system was reduced by 88.36% and 83.88%, respectively.

For vehicular cloud environments, secure Elliptic Curve Cryptography (ECC) as well as biometric-based authentication Vinod Kumar et al. [13] developed framework based on smartphones**.** In this regard, the authentication was performed based on biometric templates. Once authentication was done, the ECC algorithm encrypted the transmitted data. The system had a communication cost of 864 bits, which was better than existing methods. Jianfei presented a Privacy-preserving Data Share Mechanism with Flexible Cross-domain authorization (PDSM-FC) in autonomous vehicle systems **Sun *et al.* [14].** PDMS-FC was a ciphertext conversion technique that converted the original data into ciphertext. So, it offers effective access for all entities by holding legitimate authorization. For vehicle-data sharing in cloud computing, Nyamsuren Vaanchig et al. [15] constructed a secure-channel free identity-based encryption with equality test (IBEET)**.** The author used the ElGamal encryption and identity-based encryption methods for secure data transmission.

For vehicular networks, **Chaofan Di and Wanqing Wu [16]** presented an identity-based mutual authentication scheme. The identity-based cryptography (IBC) was used to generate keys for secure communication, solving the key escrow issue occur during transmission. The system showed the results that took less execution time of 57.2867ms than the existing methods. A confidentiality preserving authentication protocol was suggested by **Kumar Prateek *et al.* [17]** for vehicular networks**.** Primarily, the registration was done by providing the vehicle exclusive identify with a trusted authority (TA). Then, both TA and vehicle carry out quantum key replace protocol for secure data transmission. The results showed that the system has a less communication cost of 2864bits.

Mahmood A. Al-Shareeda *et al.* [18] presented a secure model for fifth-generation vehicular networks without RSU. The system used pseudonym-identity generation to generate the pseudonym-ID and the signature key for secure data sharing. The system reduced the message-signature-tuple size and communication overhead by 13.89%. Hybrid cryptography was suggested by **Walter Tiberti *et al.* [19]** to secure intra-vehicle communications.

The system used the Elliptic Curve Topology-Authenticated Key Scheme (ECTAKS) element to perform encryption, distribution, key generation, and signature management through NIST-compliant elliptic curves. The method achieved an encryption and decryption times in the range between 0.73 and 0.87 and 0.59 and 0.73ms, which shows its better performance over other similar models.

A blockchain based vehicular data sharing system was suggested by **Junqin Huang *et al.* [20]**. The identity privacy of the vehicles was protected using zero-knowledge proof technology to preserve the auditability of the vehicular data for trusted authorities. Then, blockchain mechanism was utilized to store the data to protect it from the attacker. The results showed that the system taken less running time of 2.1 ms. For VCC, **Vinod Kumar [21]** suggested a secure framework based on biometric. The system performed biometric based authentication to verify the legitimate users and then, it used an elliptic curve cryptography (ECC) algorithm for secure data transmission. The results showed that the system was secure regarding communication and computation overheads.

For vehicular networks**, Jing Zhang *et al.* [22]** presented a secure data sharing scheme based on revocable cache. The system used ciphertext-policy attribute-based encryption (CP-ABE) to securely transmit the data in the cloud. The system achieved superior balance betwixt and communication and computational costs compared to related works. A lightweight trust-based system was proposed by **Sandeep Kumar Arora *et al.* [23]** for vehicular network using blockchain. The smart contracts and the blockchain mechanisms were used by the system for the local vehicles, which offered better two-way authentication and reduced the overheads. The system also prevented the network form being stolen it avoided third parties from being attacked by third parties as a result, network privacy was increased. The system taken less message authentication cost of 1024 bits.

A hybrid mechanism was suggested by Righa Tandon and P.K. Gupta [24] for vehicular networks. During inter-vehicle communication, the system hybridized digital signature and advanced encryption standard for securing the vehicular data. The obtained outcomes represented that the system reduced the network's overall time-delay.

2.1 Research Gaps

The above-mentioned works provide better solutions to offer security to the vehicular cloud system. Most of the above works only concentrate on authentication to provide security. It didn't help to protect the confidential information and sensitive data. The important part is encryption, since an unauthorized person or creature can get access when the data is encrypted, yet they will not be able to read it. The author [10] uses the Block cipher algorithm to encrypt the vehicle information for cloud storage.

A block cipher is a symmetric encryption algorithm that has high diffusion and tough tamper resistance, however, both sender and receiver should have the same access key, that makes the key management process challenging. All the encrypted data are at high risk when the key is misplaced or compromised. The author [11-13, 15] uses the RSA, ECC, and Elgamal encryption algorithms for encrypting the data, which are asymmetric and it utilizes two keys such as private key as well as public key.

For encryption, public key is used and for decryption, private key is used. Those two keys are selected randomly and these key generations enlarge computational process complexity and reduce the performance of encryptions. Considering these challenges, for VCC, this paper proposes an optimal data-sharing method using an optimized RSA algorithm for performing secure communication in VCC.

3. PROPOSED METHODOLOGY

Figure 2 shows the cryptographic process of proposed ORSA for secure data-sharing in VCC. The proposed RSA algorithm consists mainly three phases: key generation, encryption, and decryption. The key generation process in RSA is done using COA approach, which optimally chooses the public key instead of random key selection. These phases are briefly explained in the following section.

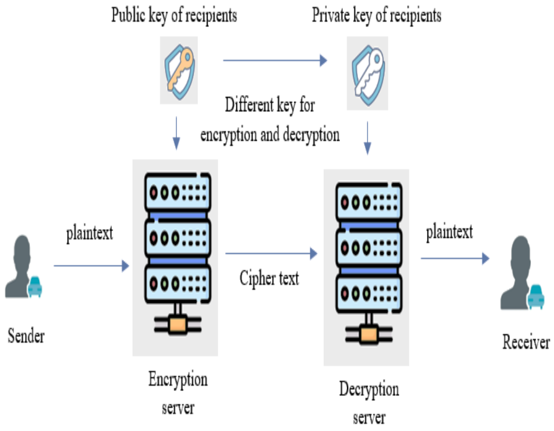


Figure 2: Cryptographic process of ORSA

3.1 Secure Data Transmission

To securely transmit vehicle information to the cloud, authentication is essential. For authorizing the vehicles, they must register with the RSU and their information is transmitted to the cloud once their authorization is successfully completed by the RSU. After the registration step, the vehicle and RSU agree to generate the key for secure communication among the RSU and other onboard units (OBUs). The vehicle and RSU are verified by a trusted authority (TA), and the vehicles and RSU can transmit the data to the cloud only if the TA checks that they are legitimate entities. The data is securely transmitted to the VCC by encrypting it using an ORSA model.

RSA is a widely used asymmetric key cryptography algorithm that increases data communication security. The model has three main phases: key generation, encryption, and decryption. Firstly, the input data was transmitted into ciphertext using a public key. Extracting the original text from the ciphertext within a reasonable time is considered infeasible without a password. Secondly, the decryption process was done to restore the ciphertext from its original plaintext by utilizing a private key.

The RSA algorithm was the most widely used method for securing data because the mathematical equations used there were difficult to hack. In RSA, the key generation plays a vital role in strengthening security. The key generation process in RSA uses a pseudo-random number generator. However, distribution needs to more consistent for higher amounts of produced numbers. Additionally, they use predictable pseudo-random numbers, which cannot be utilized for data encryption. Hence, the proposed system uses a spiral Learning-centered Coati Optimization Algorithm (SLCOA) to select the public key optimally. Then, the optimal public key-based private key is selected for further processing. Thus, the optimal key generation selection in primary RSA is called ORSA. The steps involved in the ORSA were explained as follows:

i) Key generation

In the RSA algorithm, the initial stage is to generate the key, which involves a public and private key. A public key is considered an open key that is visible to everyone and used for encrypting messages, and a private key performs decryption. The RSA algorithm first, chooses two distinct large random prime numbers $\hat{X}$ and $\hat{Y}$. Then computes $\hat{W}_F = \hat{X} . \hat{Y}$, where, $\hat{W}_F$ is used as the modulus for both public and private keys. After that, calculate the Euler totient function ($\ddot{\xi}$) of $\hat{W}_F$ using equation (3).

$$\ddot{\xi}\left(\hat{W}_F\right) = \left(\hat{X} - 1\right) * \left(\hat{Y} - 1\right) \qquad (1)$$

After that, the public key is randomly generated between the ranges of 1 to $\ddot{\xi}\left(\hat{W}_F\right)$ for encryption. This random generation of public keys takes more time and is easily predictable by third parties. To mitigate these deficiencies, this article proposes the SLCOA algorithm to optimally select the public key that prevents the network from third-party attacks. COA is a new nature-inspired optimization algorithm that mimics coati behavior by establishing a phase's exploitation and exploration. In the group of coatis, half of the coatis wait under the tree while the other half climb above the tree to terrify the prey. Additionally, coatis abandon their prediction attempts and flee when they encounter predators.

By observing these behaviors of coatis to balance exploration and exploitation in a search process, the COA algorithm aims to attain efficient optimization. During the exploration phase, the prey's position falling from the tree was randomized, showing the algorithm's slow convergence speed. Conversely, when coati approached prey, it easily fell into local optimal in a later stage. Thus, the algorithm's performance was reduced. So, the proposed system uses a spiral learning strategy to avoid the local optima issues and increase the global search ability. This improvisation in the traditional COA is termed SLCOA. The process implicated in the proposed is known as follows:

At the start of the COA execution, the coati's position in the search space is randomly initialized using equation (2).

$$\hat{D}_k : \hat{D}_{k,l} = LB_l + \ddot{R}_N . \left(UB_l - LB_l\right), \quad k = 1,2,\ldots N, \quad l = 1,2,\ldots.n \qquad (2)$$

Where, $\hat{D}_k$ specifies the k^{-th} coati's position in the initialized search space, $\hat{D}_{k,l}$ denotes the l^{-th} decision variable's value, n indicates the number of decision variables, N signifies the number of coatis, $\ddot{R}_N$ signifies a arbitrary real number between [0, 1], and UB_l & LB_l specifies the upper and lower bound of the l^{-th} decision variable, respectively.

After that, each individual's fitness was estimated and the COA positions were updated in two phases: exploration and exploitation. The coati contains two groups that perform the exploration. The first group scares the prey by climbing the tree, and the second waits for the falling scared prey by staying under the tree. The position of the coatis is expressed mathematically by equation (5).

$$\hat{D}_k^{P1} : \hat{D}_{k,l}^{P1} = \begin{cases} \hat{D}_{k,l} + \hat{L}_S . \left(prey_l^A - \ddot{J}_M . \hat{D}_{k,l}\right), & \ddot{E}_{prey^A} < \ddot{E}_k \\ \hat{D}_{k,l} + \hat{L}_S . \left(\hat{D}_{k,l} - prey_l^A\right), & Else \end{cases} \qquad (5)$$

Where, $\hat{D}_k^{P1}$ represents the k^{-th} coati's new position, $\hat{D}_{k,l}^{P1}$ refers to the coati's position in the l^{-th} dimension, $\ddot{J}_M$ specifies an arbitrary integer value, $prey_l^A$ refers to the prey's position in the l^{-th} dimension, and $\hat{L}_S$ specifies the strategy of spiral learning that accelerates the coati to move central point and decreases the step size gradually in the movement, which increases the model's global search ability. It is given in equation (6).

$$\hat{S}_L^F = \hat{D}_{k,l} * e^{\alpha\mu} * \cos\left(2\pi\mu\right) \qquad (6)$$

Where, μ represents the random number and α denotes the logarithmic helix coefficient, respectively. Next, in the exploitation phase, when a predator attacks a coati, it moves to a random position near to it according to equation (7).

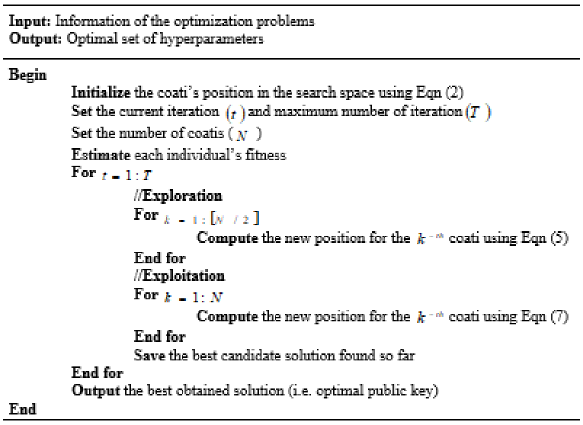
$$\hat{D}_k^{P2} : \hat{D}_{k,l}^{P2} = \hat{D}_{k,l} + \left(1 - 2\hat{L}_S\right) . \left(\frac{LB_l}{t} + \hat{L}_S . \left(\frac{UB_l}{t} - \frac{LB_l}{t}\right)\right), \qquad (7)$$

Where, t is the current iteration. After updating the all-coatis' position in the search space, an iteration of SLCOAs is stopped. In this way, the optimal public key is selected for encryption. Then, the private key is generated using equation (8).

$$\hat{P}_{RK} = \left(\hat{P}_{UK}\right)^{-1} \bmod \ddot{\xi}\left(\hat{W}_F\right) \qquad (8)$$

Where, $\hat{P}_{RK}$ indicates the private key and $\hat{P}_{UK}$ specifies the optimal public key generated using SLCOA.

The pseudocode of the proposed SLCOA is given in Figure 3.



```
Input: Information of the optimization problems
Output: Optimal set of hyperparameters

Begin
        Initialize the coati's position in the search space using Eqn (2)
        Set the current iteration $(t)$ and maximum number of iteration $(T)$
        Set the number of coatis $(N)$
        Estimate each individual's fitness
        For $t = 1 : T$
                //Exploration
                For $k = 1 : [N/2]$
                        Compute the new position for the $k^{th}$ coati using Eqn (5)
                End for
                //Exploitation
                For $k = 1 : N$
                        Compute the new position for the $k^{th}$ coati using Eqn (7)
                End for
                Save the best candidate solution found so far
        End for
        Output the best obtained solution (i.e. optimal public key)
End
```

Figure 3: Pseudocode of the proposed SLCOA

ii) Encryption

In the encryption process, a readable message is converted into an unreadable form so that unauthorized parties cannot read it. The steps used for encrypting the vehicle information are given as follows:

Step 1: The cloud service provider transmits the public key to the user for data storage within the server.

Step 2: To record the user data into an integer, a reversible protocol is used, which is known as a padding scheme.

Step 3: The data is encrypted using the sender's public key, and the resultant cipher data $(\ddot{C}_T)$is obtained using equation (9).

$$\ddot{C}_T = \left(\hat{I}_{VD}\right)^{\hat{P}_{UK}} \bmod \hat{W}_F \tag{9}$$

Where, $\hat{I}_{VD}$ indicates the input data, and $\hat{P}_{UK}$ represents the public key.

Step 4: Finally, the encrypted data was stored in the cloud.

Decryption

Decryption converts an encrypted message reverse to its original (readable) format. The steps for decrypting the data are as follows:

Step 1: The cloud service provider asks for the private key to verify the authenticity of the user if they request data access in the cloud. Once verified, the encrypted data i.e., $(\ddot{C}_T)$is provided to the user.

Step 2: Decryption is done by the user using the following equation (10). The pseudocode of the proposed RSA is shown in fig. 4.

$$\hat{I}_{VD} = \left(\ddot{C}_T\right)^{\hat{P}_{RK}} \bmod \hat{W}_F \tag{10}$$

```
Algorithm: Optimized RSA for secure VCC communication

Key Generation
Initialize two random large prime numbers as $\hat{X}$ and $\hat{Y}$
Compute $\hat{W}_F = \hat{X} \cdot \hat{Y}$
Estimate Euler's totient function as
        $\ddot{\xi}(\hat{W}_F) = (\hat{X} - 1) * (\hat{Y} - 1)$
Generate the public key $\hat{P}_{UK}$ by applying SLCOA
Generate private key $\hat{P}_{RK}$ such that $\overline{PR}_{key} = \hat{P}_{UK} - 1 \ (mod \ \ddot{\xi}(\hat{W}_F))$
Encryption
        Compute $\ddot{C}_T = (\hat{I}_{VD})^{\hat{P}_{UK}} \ mod \ \hat{W}_F$
The function uses the public key components as $\hat{W}_F, \hat{P}_{UK}$ , and plain text as $\hat{I}_{VD}$
Decryption
        Compute $\hat{I}_{VD} = (\ddot{C}_T)^{\hat{P}_{RK}} \ mod \ \hat{W}_F$
The function uses the public key components as $\hat{W}_F, \overline{PR}_{key}$, and cipher text as $(\ddot{C}_T)$ to get
original message
```

Figure 4: Pseudocode of proposed RSA

4.RESULTS AND DISCUSSION

Here, the performance effectiveness of the proposed optimal RSA system for secure data transmission in VCC is analyzed by comparing its outcomes with those of the existing systems regarding some performance measures. The proposed research model is implemented in Java with Windows 10 OS, 12 GB RAM, and Intel(R) Core (TM) i5-5200U Processor (3M Cache, 2.20 GHz). The simulation parameters of the proposed system for secure communication in VCC are listed as follows.

Table 1: Simulation parameters

Parameters	Values
Topology (m^2)	5000 × 5000
Number of nodes	200
Number of RSUs	4
communication range of nodes (m)	300
Speed (m/s)	30
MAC layer	MAC 802_ 11p
Time (s)	300

The existing methods considered for comparison are AES, Diffie Hellman (DH), and Blowfish (BLF), and the performance measures considered for comparing the effectiveness of the proposed as well as existing techniques are encryption time, decryption time, reliability, network lifetime (NLT), packet delivery ratio (PDR), communication cost, storage cost, and energy consumption. These metrics definitions are shortly described as follows:

a) Encryption time

It is the difference between the encrypting completed time $\left(\breve{E}_{CT}\right)$and the initiated time $\left(\breve{E}_{IT}\right)$. It is defined as follows:

$$Encryptiontime = \breve{E}_{IT} - \breve{E}_{CT} \tag{11}$$

b) Decryption time

It is the difference between the time taken to convert ciphertext into the original text $\left(\breve{Đ}_{CT}\right)$and the initial time $\left(\breve{Đ}_{IT}\right)$. It is formulated as follows:

$$Decryption\ time = \breve{Đ}_{IT} - \breve{Đ}_{CT} \tag{12}$$

c) Reliability

Reliability metrics are used to quantitatively express the reliability of the transmitted data to the cloud.

d) NLT

It measures network's lifespan which indicates the dying time of the first node in the network. It is expressed as follows:

$$NLT = \frac{\overleftrightarrow{I}_{ER} - \overleftrightarrow{W}_{ER}}{\overleftrightarrow{C}_{PC} + \overleftrightarrow{\zeta}_{M}\ \overleftrightarrow{R}_{ES}} \tag{13}$$

Where, $\overleftrightarrow{C}_{PC}$ denotes network's continuous power consumption, $\overleftrightarrow{I}_{ER}$ denotes network's initial energy, $\overleftrightarrow{W}_{ER}$ indicates wasted energy, $\overleftrightarrow{\zeta}_{M}$ represents reporting time of average vehicular node, and $\overleftrightarrow{R}_{ES}$ denotes assessed reporting energy.

e) PDR

It is the ratio of amount of received packets $\left(\overleftrightarrow{S}_{RP}\right)$and total amount of data packets transmitted$\left(\overleftrightarrow{T}_{NP}\right)$. It is defined as follows:

$$PDR = \frac{\overleftrightarrow{S}_{RP}}{\overleftrightarrow{T}_{NP}} \tag{14}$$

f) Communication cost

It is a cost and is estimated based on the amount of data transmitted between different vehicle users.

g) Storage cost

The amount of memory units required by the model to perform encryption operation is referred to as storage cost.

h) Energy consumption

Energy consumption metric is described as the amount of energy consumed by vehicular network for data sensing, transmitting and receiving. It is formulated as follows:

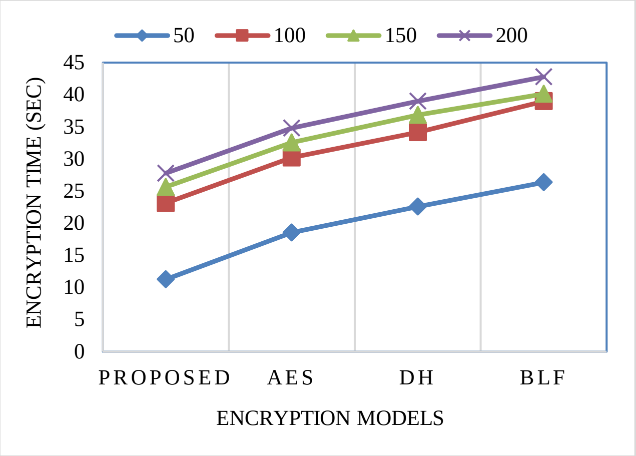
$$Energyconsumption = \sum \tilde{\eta}_{ST} + \tilde{\eta}_{M} \tag{15}$$

Where, $\tilde{\eta}_{ST}$ represents the energy consumed during data transmission and $\tilde{\eta}_{M}$ represents the energy consumed during data receiving.Table 2 shows the encryption and decryption time outcomes of the proposed as well as existing approaches.

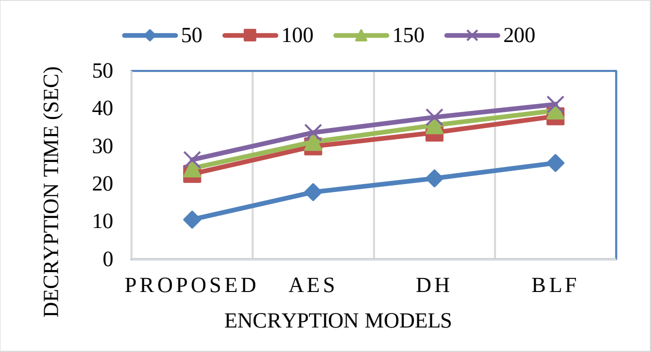
Table 2: Encryption and decryption time analysis

Metrics	No of Vehicle nodes	Proposed	AES	DH	BLF
Encryption time (s)	50	11.25	18.56	22.56	26.35
	100	23.14	30.23	34.15	38.97
	150	25.64	32.56	36.85	40.12
	200	27.79	34.81	38.97	42.78
Decryption time (s)	50	10.54	17.79	21.45	25.56
	100	22.64	29.98	33.65	37.97
	150	24.13	31.13	35.54	39.47
	200	26.41	33.64	37.74	41.13

Encryption time is the time the encryption method takes to convert the actual data into encrypted data. In contrast, the decryption time is the time the cryptographic approach takes to convert the encrypted data into actual data. The encryption and decryption time of the approaches are measured by varying the number of vehicular nodes in VCC from 50 to 100. For 50 nodes, the existing methods say RSA, AES, DH, and BLF take 14.23s, 18.56s, 22.56s, and 26.35s time to encrypt the data and 13.21s, 17.79s, 21.45s, and 25.56s time to decrypt the data, which are comparatively higher than the proposed one because the proposed one takes less encryption and decryption time of 11.25s and 10.54s for the same 50 nodes of vehicle data. Similarly, for the remaining number of nodes 150-200, the proposed model takes less encryption and decryption time than the existing methods. Because the key generation process of the RSA is done optimally and uses more minor keys for encryption and decryption than other existing models, it results in quick data processing. The diagrammatic illustration of table 2 is shown in fig.5.



(a)



(b)

Figure 5: Encryption and decryption time analysis

Then, the reliability analysis of the proposed and existing methods is done, as shown in Figure 2. Reliability indicates the security level the encryption models offer for reliable communication between the vehicular nodes in VCC. Our model shows higher reliability than the existing systems; for example, for a maximum of 200 nodes, the proposed one has a better reliability of 96.94%, which is 5.1%, 6.20%, and 8.19% higher than the AES, DH, and BLF. Because the mathematical complex cryptographic processes in RSA are challenging to crack by the third parties. Thus, the results confirm that the proposed method achieves superior outcomes compared to the existing methods.

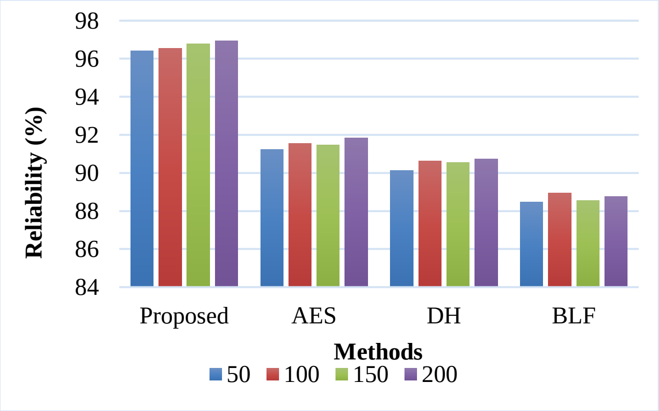


Figure 6: Reliability analysis

Table 3: NLT analysis

Metrics	No of Vehicle nodes	Proposed	AES	DH	BLF
NLT (h)	50	121	101	89	75
	100	126	108	96	82
	150	128	105	93	79
	200	147	129	117	103

Table 3 illustrates the efficiency of the proposed and the existing methods regarding NLT. In a VCC, NLT is considered as the important one to maintain a connection between the vehicular nodes. It needs to be high to show the effectiveness of our model with minimal energy consumption. For example, for 50 nodes, the existing BLF has less NLT of 75h than the other existing methods and the proposed one. The proposed one has high NLT of 121h for the same 50 nodes. Similarly, for the remaining no of nodes, the proposed one has more NLT. Thus, it shows the effectiveness of the proposed model. It is also graphically shown in Figure 7.

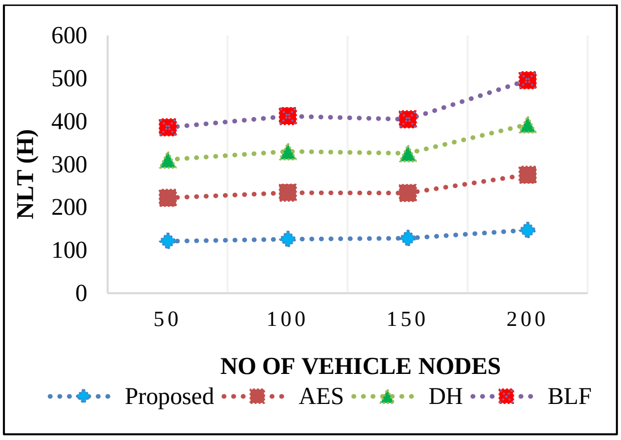


Figure 7: NLT analysis

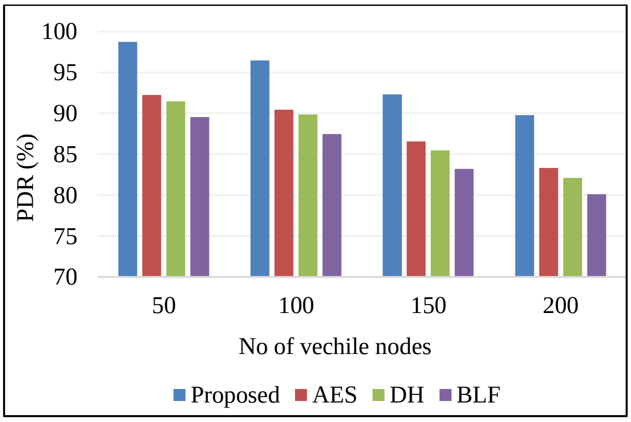


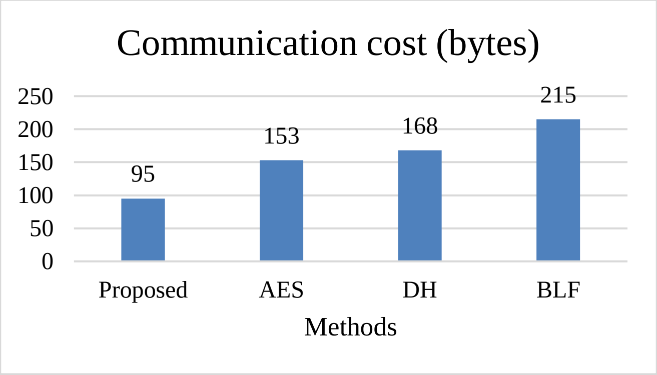
Figure 8: PDR analysis

Figure 8 demonstrates the outcomes of the proposed model based on PDR metric. In this figure, the proposed model achieves high PDR than the existing methods for all the no of vehicle nodes. For example, the proposed one achieves high PDR of 98.74%, 96.45%, 92.34%, and 89.78% for 50-200 nodes, which is higher when compared to the existing methods. Thus, it proves that the proposed one outperformed existing method.

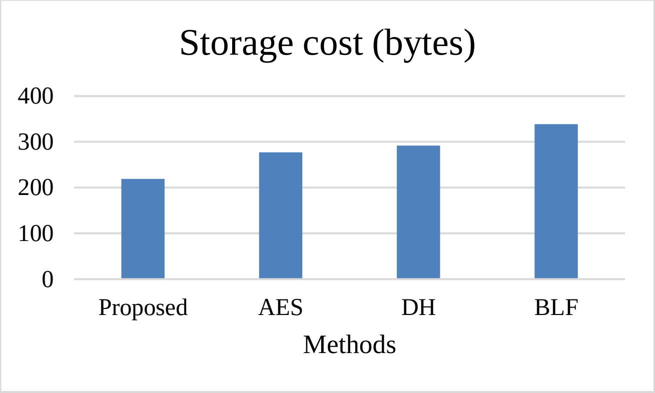
Table 4: Results analysis of the proposed model

Methods	Communication cost (bytes)	Storage cost (bytes)	Energy consumption (mJ)
Proposed	95	219	0.172
AES	153	277	0.289
DH	168	292	0.386
BLF	215	339	0.478

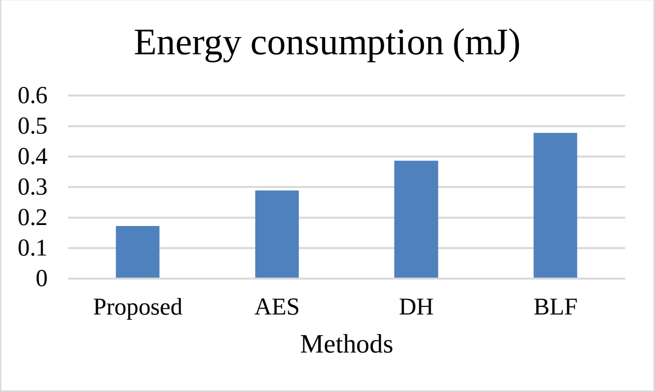
Table 4 illustrates the results of the proposed and existing models regarding communication cost, storage cost, and energy consumption. Considering the communication cost, the existing models have 125 bytes, 153 bytes, 168 bytes, and 215 bytes, which are higher than the proposed one because it has a communication cost of 95 bytes. Considering other metrics, the proposed one also has less storage cost of 219bytes and consumes less energy of 0.172mJ, which is better than the existing methods. The reason is that ours is an effectual and optimal asymmetric encryption algorithm. It assures confidentiality, integrity, and authenticity. The public key is optimally chosen by the SLCOA method, in which the convergence speed is increased via a spiral learning strategy, which leads to better results for the data security of the VCC system regarding the measures mentioned above. The graphical demonstration of table 4 is shown in fig.9.



(a)



(b)



(c)

Figure 9: Analysis based on communication cost, storage cost and energy

5. CONCLUSION

This paper proposes a secure data-sharing scheme for VCC using an ORSA algorithm. In experimental analysis, the efficiency of the proposed model is weighted against the traditional AES, DH, and BLF algorithms based on encryption time, decryption time, reliability, communication cost, storage cost, and energy consumption metrics. The evaluation is carried out for vehicle nodes ranging from 50 to 200. For 50 nodes, the proposed model takes 11.25s and 10.54s for encryption and decryption, achieving 96.41% reliability for the same node. Also, it takes less communication cost of 95bytes, storage cost of 219bytes, and consumes less energy of 0.172mJ. Likewise, the proposed method attains better outcomes for the remaining nodes than the existing methods. It was observed that the optimal version of RSA showed more satisfactory results and proved its security and reliability compared to the conventional algorithms. This work will be prolonged in the future with another fast and effective asymmetric-based encryption system with a resource allocation strategy to offer secure and effective cloud storage.

REFERENCES

[1] Quy, V. K., Nam, V. H., Linh, D. M., Ban, N. T., & Han, N. D. (2022). Communication solutions for

vehicle ad-hoc network in smart cities environment: A comprehensive survey. *Wireless Personal Communications*, *122*(3), 2791-2815.

[2] Gong, M., Yoo, Y., & Ahn, S. (2023). Vehicular Cloud Forming and Task Scheduling for Energy-Efficient Cooperative Computing. *IEEE Access*, *11*, 3858-3871.

[3] Alhilal, A. Y., Finley, B., Braud, T., Su, D., & Hui, P. (2022). Street smart in 5G: Vehicular applications, communication, and computing. *IEEE Access*, *10*, 105631-105656.

[4] Shahnawaz, A., & Shabana, M. (2024). Efficient time-oriented latency-based secure data encryption for cloud storage [J]. *Cyber Security and Applications*, *2*, 100027.

[5] Akilandeswari, V., Kumar, A., Thilagamani, S., Subedha, V., Kalpana, V., Kaur, K., & Asenso, E. (2022). Minimum latency-secure key transmission for cloud-based internet of vehicles using reinforcement learning. *Computational Intelligence and Neuroscience*, *2022*.

[6] Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. *Big Data and Cognitive Computing*, *6*(4), 101.

[7] Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. *Computers and Electrical Engineering*, *102*, 108205.

[8] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.

[9] Sana, M. U., Li, Z., Kiren, T., Liaqat, H. B., Naseem, S., & Saeed, A. (2023). A Secure Method for Data Storage and Transmission in Sustainable Cloud Computing. *Computers, Materials & Continua*, *75*(2).

[10] Boubaker, S., Alsubaei, F. S., Said, Y., & Ahmed, H. E. (2023). Lightweight Cryptography for Connected Vehicles Communication Security on Edge Devices. *Electronics*, *12*(19), 4090.

[11] Al-Balasmeh, H., Singh, M., & Singh, R. (2022). Framework of data privacy preservation and location obfuscation in vehicular cloud networks. *Concurrency and Computation: Practice and Experience*, *34*(5), e6682.

[12] Liu, Z., Wan, L., Guo, J., Huang, F., Feng, X., Wang, L., & Ma, J. (2023). PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks. *IEEE Transactions on Vehicular Technology*.

[13] Kumar, V., Al-Tameemi, A. M. A., Kumari, A., Ahmad, M., Falah, M. W., & Abd El-Latif, A. A. (2022). Psebvc: Provably secure ecc and biometric based authentication framework using smartphone for vehicular cloud environment. *IEEE Access*, *10*, 84776-84789.

[14] Sun, J., Xu, G., Zhang, T., Cheng, X., Han, X., & Tang, M. (2022). Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*.

[15] Vaanchig, N., Qin, Z., & Ragchaasuren, B. (2022). Constructing secure-channel free identity-based encryption with equality test for vehicle-data sharing in cloud computing. *Transactions on Emerging Telecommunications Technologies*, *33*(5), e3896.

[16] Di, C., & Wu, W. (2022). A novel identity-based mutual authentication scheme for vehicle ad hoc networks. *Wireless Communications and Mobile Computing*, *2022*.

[17] A Privacy Preserving Authentication Protocol Using Quantum ComputingforV2IAuthenticationinVehicularAdHocNetworks

[18] Al-Shareeda, M. A., Manickam, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Qtaish, A., Alzahrani, A. J., ... & Almekhlafi, K. (2022). Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU). *Sustainability*, *14*(16), 9961.

[19] Tiberti, W., Civino, R., Gavioli, N., Pugliese, M., & Santucci, F. (2023). A Hybrid-Cryptography Engine for Securing Intra-Vehicle Communications. *Applied Sciences*, *13*(24), 13024.