International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-2, December 2021

Lightweight VANET Architecture for Efficient Secure Data Transmission using CPABE & IBOOS

G. Keerthana, J. Suguna

Abstract: ***Cloud computing is a network access concept that provides simple, on-demand network access to a shared pool of customizable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provided and released with minimal administrative effort or service provider involvement. The idea of having a communication node on-board a vehicle that may make wireless connections with other adjacent communication nodes visible in the radio range is referred to as a Vehicular Adhoc Network (VANET). The main focus of this paper is to design lightweight Vehicular Adhoc Network architecture for efficient secure data transmission. An improved Ciphertext Policy Attribute Based Encryption scheme and Identity Based offline/online Signature scheme are proposed to reduce the computational cost, storage overhead and communication overhead in vehicular ad-hoc network. Finally, concluded that the proposed work yields high performance than the existing work.***

Keywords: Cloud Computing, Vehicular Adhoc Network, Ciphertext Policy Attribute Based Encryption, Identity Based offline/online Signature.

I. INTRODUCTION

Cloud Computing is the ease of access to computer resources and services through the internet [6]. By establishing the process hardware, cloud computing has the ability to alter the Information Technology (IT) sector, making both software and infrastructure more appealing as services [5].

A. Vehicular Ad-Hoc Network (Vanet)

Trusted Authority (TA), Road Side Unit (RSU), and terminal vehicles are the main components of VANET architecture. TA is in charge of critical system activities such as device registration, key generation, and vehicular data processing as the top-level VANET administrative centre and virtuous key centre [1].

Manuscript received on November 30, 2021.
Revised Manuscript received on December 11, 2021.
Manuscript published on December 30, 2021.
* Correspondence Author
Dr. J. Suguna, Associate Professor, Department of Computer Science, Vellalar College for Women, Thindal, Erode (Tamil Nadu), India.
G. Keerthana*, Research Scholar, Department of Master of Computer Application, Vellalar College for Women, Thindal, Erode (Tamil Nadu), India.

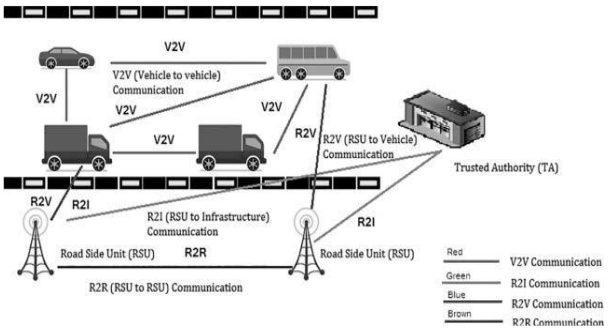

Fig. 1. Vehicular Adhoc Network

Components Of Vanet

The following are the vehicular adhoc network components:

- **On-Board Unit (OBU):** On-board unit provide processing of their own vehicle data, traffic data, and other vehicle-related data, and thus help to take a decision in various real-life applications like congestion control and accidents prevention. An OBU should track the position of the vehicle and the distance it travels. An OBU should offer a connection with other OBUs and RSUs.
- **Road-Side Unit (RSU):** RSUs verify all broadcasted messages and transactions before they are registered in the blockchain. RSUs are also in charge of updating the authentication data held in each vehicle via vehicle-to-infrastructure communication (Fig.1) [14].
- **Trusted Authority (TA):** Trusted authority server is the main server to keep records of VANET such as RSUs, vehicles, and OBUs. Also, it is responsible to authorize these RSUs and vehicles, after that only, RSUs or vehicles can communicate in a vehicular network (Fig.1).
- **Vehicle:** The blockchain is used to provide a privacy-preserving authentication method between automobiles. On the one hand, automobiles may monitor TA and law enforcement agencies by authenticating all blockchain transactions. The worldwide consensus, on the other hand, is based on the Proof of Work (PoW) produced by cars. [14].

B. Vehicular Cloud Computing

Excess processing power may now be used due to the cloud computing concept. The massive number of automobiles on city streets, highways, and parking lots will be considered as underutilized computing resources that may be employed to provide public services [10].

The goal of vehicular computing has to provide services to automobiles that increase traffic safety and efficiency. The vehicular cloud has the possible to completely revolutionise the way we communicate in automobiles. Cars' underutilized resources might be expressly divided with further vehicles reaching control traffic in congested areas. Storage, computational power and internet connectivity are just a few of the resources available [2].

C.Types Of Vehicular Cloud Computing

There are three types of vehicular clouds: Vehicle to Vehicle clouds (V2V clouds), Vehicle to Infrastructure clouds (V2I clouds), and vehicular clouds mixed with other commercial clouds (integrated clouds) [10].

Vehicle to Vehicle Cloud: Vehicle-to-Vehicle transmission's ability to wirelessly interchange information on the speed and location of neighboring cars has huge promise for decreasing traffic congestion, averting collisions, and improving the environment [2].

Vehicle-to-Infrastructure Cloud: Vehicle-to-Infrastructure (V2I) refers to data interchange between automobiles and fixed network infrastructures. In most situations, these interactions entail Road-Side Units (RSU) and gateways providing access to external networks, similarly the Internet or other typical cloud service. V2I communication links provide greater security, but they require more bandwidth than V2V communication links.

Integrated vehicular clouds: While additional clouds, similarly mobile computing and also Internet clouds, are linked to vehicular and integrated clouds arise. Whether the cloud is coupled with the Internet cloud to Global Positioning System (GPS) and other utilities, it is referred as an Internet based vehicular cloud, and if it uses the services of commercial clouds like as Google and Amazon, it is referred to as a services-dependent integrated cloud [2].

D. Attribute Based Encryption

Attribute Based Encryption (ABE) referred as a form of public encryption. ABE is provided to protect data transported via a network. Sahai and also Waters [3] pioneered the use of attribute based encryption to achieve access control through public key cryptography. The ABE technique is used in log encryption. In the event of encrypting each portion of the log with the keys of all receivers, it is possible to encrypt the log with the matching recipients attribute. If only the attribute matches the ciphertext and the user's secret key and finally the end-user can decrypt the ciphertext. The primary objective is to provide scalability, flexibility, and safe access control. Both the ciphertext and the user secret key are connected with a pair of characteristics in the ABE scheme. There are several concepts offered in terms of security and speedy decryption. Because it is based on the user's traits, the ABE method is well-known for electronic transactions. This technique is commonly employed in vector-driven search engines.

Challenges

Although the ABE idea is a highly strong and promising mechanism, ABE systems have two major drawbacks: inefficiency and the lack of an attribute revocation mechanism.

Other major problems include:

- Key coordination
- Key escrow
- Key revocation

The remaining of the research work is structured as follows. Section II explains the relevant researches briefly. Section III provides the details of entire system architecture. Section IV elaborates the experimental solutions and its discussions. Section V terminates the research work.

II. RELATED WORK

The various existing literatures related to VANET Architecture are studied in order to identify the suitable method for secure Data Transmission.

Hong Zhong et al., [15] introduced a safe strategy for sharing data between domains based on edge computing. In accordance with the notion of edge computing, the cars are chosen to operate as nodes. Elliptic Curve Cryptography (ECC) and Ciphertext Policy Attribute Based Encryption (CPABE) are employed to maintain the secrecy of the information, and the scheme's security and efficiency are demonstrated.

Juan Wang et al., [1] has proposed a method for vehicle-to-vehicle communication based on Lightweight Authentication (LIAU). To ensure the security of message transmission, the LIAU system employed the hash operation. It has also included a limited number of configurable parameters to save storage space and operation time. According to the performance analysis, the LIAU scheme can withstand typical security in a vehicle adhoc network.

Sherif A. Hammad et al., [9] has provided a comprehensive review of the most recent security and privacy standards in Vehicular Ad-hoc Networks (VANET). There is also taxonomy of the numerous VANET attacks depending on the communication system levels. In addition, a brief overview of the most prevalent vehicular cloud assaults and attackers has been provided. This article intends to give useful information regarding VANET security and privacy.

Sheng Ding et al., [11] studied the problem of Ciphertext Policy Attribute Based Encryption (CPABE) has now been explored as a bottleneck restricting its development and deployment. Elliptic Curve Cryptography was used to provide a unique pairing-free data access control system based on CPABE (ECC). The total computing burden for users is decreased by substituting the expensive bilinear pairing with simple scalar multiplication on elliptic curves. A new method of key distribution is being developed. According to the security and performance studies, the system considerably enhanced overall efficiency while also ensuring security.

Gaoxiang Zhang et al., [7] reviewed security concerns against the crowd sensing mechanism in Vehicle-to-Everything (V2X) networks were presented, as well as why existing safeguards fail to address these vulnerabilities. The potential of two V2X-specific attacks resulting to platoon deviation or mistakes in the vehicle's trajectory is examined, which may risk road safety further.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The debate concludes with countermeasures such as introducing a security sub-layer to V2X network protocols to give privacy, authentication, and secrecy to V2X users.

Mani Zarei et al., [8] presented an analytical model that studies vehicle mobility in a single direction of a free-flow highway mathematically. The model proposed explores a strategy in which time is divided into equal-length periods and each vehicle can adjust its speed at the start of each time slot. Simulation is used to validate the accuracy results. The results give useful insights for creating new apps and enhancing the performance of current ones over a vehicle adhoc network.

Jin Feng Lai et al., [4] proposed data exchange system for a Vehicular Adhoc Network (VANET) that supports both fast key-updating and dynamic characteristics. To provide safe key generation and quick key-updating in dynamic VANET, the Symmetric Balanced Incomplete Block Design (SBIBD) and the idea of indistinguishability obfuscation are developed. Meanwhile, the performance and security analyses show that the suggested approach is suitable for VANET.

III. METHODOLOGY

The main objective of this work is to produce highly efficient result for secure data transmission by using Ciphertext Policy Attribute Based Encryption (CPABE) and Identity Based offline/online Signature (IBooS) scheme in VANET.

The following figure Fig. 2. shows the complete architecture of the proposed system.

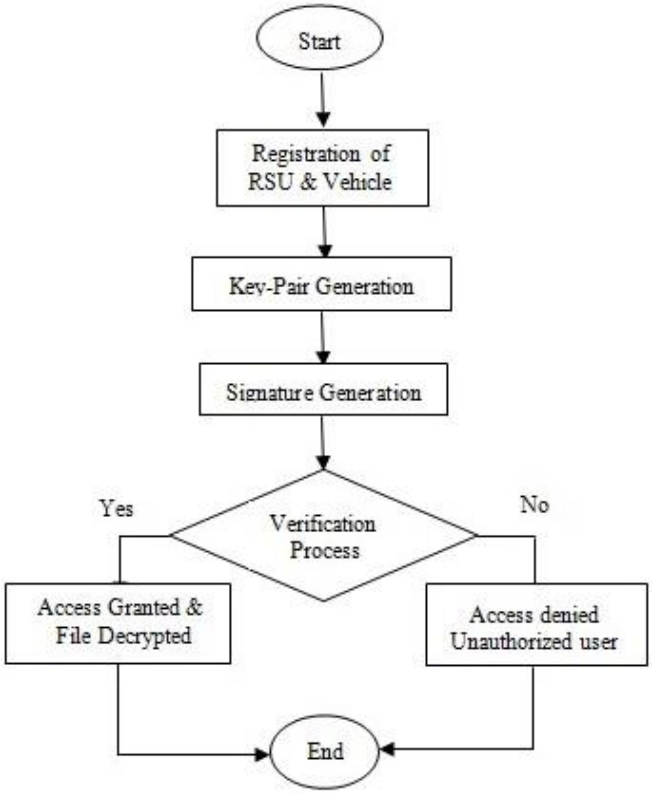

Fig. 2. System Architecture

This section, introduces the proposed lightweight Vehicular Adhoc Network (VANET) architecture, which is shown in Fig.3. The VANET architecture is made up of four entities, namely a Central Controller (CC), Content Server (CS), Road Side Unit (RSU) and Vehicle ($V_{1,2,..n}$) respectively. The improved architecture promotes the service quality of the data communication in VANET. The following are descriptions of these entities.

Central Controller (CC): It is powerful and service controller over the VANET system. The CC is constantly online and is overseen by a government entity. The parameter is initialized by the CC, which also produces the system master key and public key. The CC handles the joining and removal of road side units, as well as the registration of vehicles. It sends the signature along with the key to the user.

Content Server (CS): The Content Server is responsible for providing services to the roadside unit and car. The CS controls an attribute list based on the services it delivers; the list also contains service users. The CS encrypts service data using ciphertext attribute policy to specify who can decrypt and keep the data. The CS also handles the user's requests for services that correspond to the attribute key of the user [16].

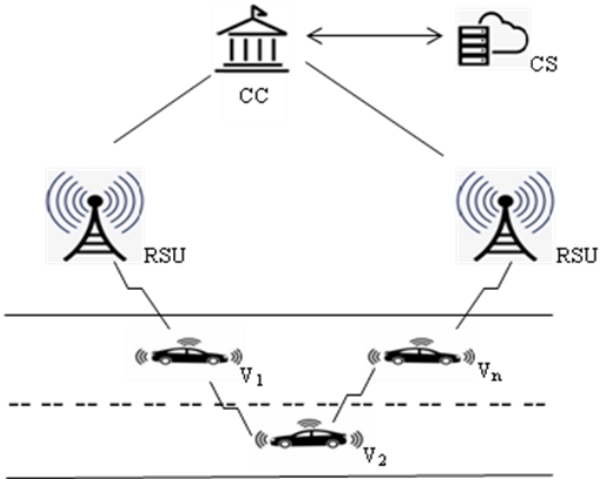

Fig. 3. Proposed Lightweight VANET Architecure

Road Side Unit (RSU): RSUs are ubiquitously deployed as edge computing devices on road sides and at junctions. An RSU is in charge of disseminating knowledge from the CC and CS to cars. Vehicles can as well as connect with one another and submit the data to CS across an RSU. RSUs further aid in the offloading of decryption calculations for the CPABE method, which was previously allocated to the on-board unit, and offer VANET with edge computing capabilities [16].

Vehicle: Vehicle is both the service user and the owner of the data, and it transfers its data to CS in encrypted structure along the help of CC [17].

A.Q-Parallel Bilinear Diffie Hellman Exponent

The primary issue with symmetric key encryption is that it requires a safe and reliable mechanism for the exchange of shared keys. The q-parallel Bilinear Diffie Hellman Exponent (QP-BDHE) key exchange, also known as exponential key exchange, is a digital encryption method that generates decryption keys based on components that are never explicitly provided.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

This protocol provides a method for using a public channel to generate a confidential shared key. In reality, the shared encryption key is based on complicated ideas such as Modular Exponentiation, Primitive Roots, and Discrete Logarithm Problems [13].

For simplicity, the scheme is provided and proved when ρ() is an injective function, however keep in mind that this simple change can allow attributes to occur at most k_{max} times with a factor of k_{max} in the private key size. The QP-BDHE problem is defined as follows. Choose a group F of prime order *p* according to the security parameter. Let a, s, $b_1,..,b_q \in Z_p$ be chosen at random and f be a generator of F_0.

If an adversary is given

$$\tilde{y} = g, g^s, g^a,...,g^{(aq)}, , g^{(aq+2)},..., g^{(a2q)}$$
$$\forall_{1\le j\le q} g^{s\text{-}bj}, g^{a/bj},...,g^{(aq/bj)},..,g^{(aq+2/bj)},...,g^{(a2q/bj)}$$
$$\forall_{1<j,k<q,k/j} g^{a\text{-}s\text{-}bk/bj},...,g^{(aq\cdot s\cdot bk/bj)}$$

It is hard to determine a valid tuple $e(g, g)^{aq+1s} \in F_T$ from a random segment $RinF_T$. An algorithm B that outputs $z \in \{0, 1\}$ has advantages ∈ in solving the decisional QP-BDHE in F_T if

$$|P_{rB}[(\tilde{y}, T = e(g, g)^{aq+1s}) = 0] - P_{rB}[(\tilde{y}, T = R) = 0]| \ge \in$$

If no polynomial time solution has a non-negligible advantage in addressing the QP-BDHE issue, the decisional QP-BDHE assumption holds [18].

B. Ciphertext Policy Attribute Based Encryption

Ciphertext Policy Attribute Based Encryption (CPABE) is a third-party data encryption mechanism that allows fine grained access control and may be used to provide a solution for secure VANET communication. Data owners can specify who has access to the shared data in CPABE. The CPABE algorithm is made up of a party encrypting data scheme that is established by a collection of attributes that constitute a policy, where the policy itself defines who can decrypt the data [16].

Setup, Encrypt, GenKey and Decrypt are four aspects executed for the VANET organization.

Setup(1^{π}): Takes as input a security parameter π. It output a Public Key P and a Master Secret Key MK.

Encrypt(P, m, A): Takes as input the Public Key PK, a Message m and an Access structure A. It outputs a Ciphertext c.

GenKey (P, MSK, S): Takes as input the Public Key PK, the Master Secret Key MK and a set of attributes S. It outputs a Secret Key SK_y.

Decrypt(P, SK_y, c): Takes as input the Public Key PK, a Secret Key SK_y and a

Ciphertext c. It outputs a Message m.

Let (P, MK) ←Setup(1^{π}), SK_y←KeyGen (P, MK, S), c← Encrypt(P, m, A). For correctness, we require the following to hold:

1. If the set S of attributes satisfies the access structure A, then m ← Decrypt (P, SK_y, c);
2. Otherwise, with overwhelming probability, Decrypt(PK, SK_y, c) outputs as unauthorized user.

C. Bilinear Pairing Algorithm

The calculation of bilinear pairing was traditionally been regarded as the most costly operation in pairing-based encryption systems. In this research, an efficient and secure outsourcing technique for bilinear pairings in the two untrusted programme model is provided. A differentiating feature of our proposed approach over the state-of-the-art technique is that the (resource-constrained) outsourcer is not needed to do any costly operations, such as point multiplications or exponentiations. This technique is also used as a subroutine to achieve outsource-secure identity-based encryptions and signatures.

Let us assume G is a state, L = Frac(G), I, J are finitely produced free G modules of the same rank, say n, and S = G –{0}. Even if the concepts that follow can be presented in greater generality, we shall operate in this setting throughout these notes.

Def 1: An G- bilinear map is an G- bilinear pairing H: I x J→G. It is worth noting that for any e∈ I, we obtain an G-linear map H*i*: J→G, where Hi = H(*i*,). As a result, Hi is a component of the dual module $Hom_G(J,G)$. We get ahomomorphism of G modules H: I → HomG from H bilinearity (J, G).

Def 2: If H: I → $Hom_G(J,G)$ is an anisomorphism of G modules, a bilinear pairing H: I x J→G is perfect.

Def 3: A non degenerate bilinear pairing H: I x J→G exists if H: I→$Hom_G(J, G)$ is injective. A perfect pairing, in particular, is nondegenerate.

Def 4: Let *i*1,...,*in*, *j*1,...,*jn* be the bases for I and J, respectively. The matrix of H, called M_H, is defined as M_H = (H(*ii*,*jj*)) for 1≤i,j≤n given a bilinear pairing H: I x J →G. Proof : Omitted.

Def 5: Let S = G –{0}. Then any bilinear pairing H : I x J → G gives a bilinear pairing $S^{-1}H : S^{-1}I \times S^{-1}J$ → K of K vector spaces.

Proof: For (i/s , j/t) ∈ $S^{-1}I \times S^{-1}J$, define $S^{-1}H$(i/s , j/t) = H(i , j) /st . Then it is quickly verified that S-1H is a bilinear map.

D. Identity Based Online/Offline Signature Scheme (Iboos)

The IBooS measure raises the effectiveness of the matching procedure by dividing the offline and online phase signature, which affirmation is relatively additional effective than IBS. An IBooS scheme from identity based cryptographic measure in VANET contains five steps they are; setup, key extraction, offline signing, online signing and verification.

- **Setup:** The central controller computes a master keys and Public Parameters P for the Private Key Generator (PK), and gives P to all vehicles.
- **Key Extraction:** The CC generates a Private Key P_K associated with the PIN using the Master Key M_K.
- **Offline Signing:** Based on the private key and public parameters, the RSU generates an Offline Signature S_{off} for each vehicle.
- **Online Signing:** Based on the Offline Signature S_{off} and a Message M_S, the sending vehicle generates an Online Signature S_{on} of M_S.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- **Verification:** Built on the PIN, M_S and S_{on}, the receiving vehicle outputs accept if S_{on} is valid for verification and otherwise output reject.

IV. RESULTS AND DISCUSSION

The result of the proposed Ciphertext Policy Attribute Based Encryption (CPABE) scheme and Identity Based offline/online Signature (IBooS) scheme is discussed and compared with the existing q-parallel Bilinear Diffie Hellman Exponent (QP-BDHE) scheme. The computational cost, storage overhead and communication overhead is reduced and cryptography cost is increased in the proposed work. The experimental results are summarized and discussed in the following section.

A. Computational Cost

Determine the execution time of the block that includes each loop and multiply it by the number of times the programme runs the loop. O is the linear time complexity of all loops that expand according to the input size (n). Even if you merely loop through half of the array, the time cost remains O(n). Time cost reflects the number of times a declaration is performed. The time cost of an code is not the actual time necessary to perform a certain code, because that is dependent on other elements, such as whatever the input, this will return in a fixed, limited period.

- CT_i - Emphasize the time taken for system initialization
- CT_e -Emphasize the time taken for encryption
- CT_k- Emphasize the time taken for key generation
- CT_d- Emphasize the time taken for decryption

Table 1. Computational Cost of QP-BDHE, CPABE and IBooS

Parameter	QP-BDHE(ms)	CPABE(ms)	IBooS(ms)
CT_i	57	52	48
CT_e	52	33	35
CT_k	43	35	28
CT_d	61	38	42

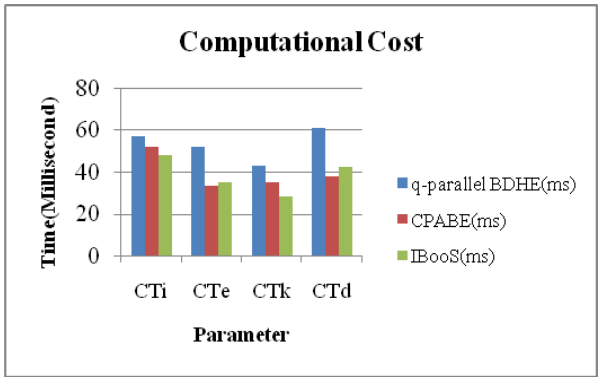

Fig. 4. Computational Cost of QP-BDHE, CPABE and IBooS

From Fig. 4, the CPABE and IBooS scheme, takes less execution time than QP- BDHE when transferring the similar amount of data and gives best presentation than the QP-BDHE scheme.

B. Storage Overhead

Storage overhead is a collection of extra memory, bandwidth, and other resources necessary to complete a certain activity. The storage overhead of the proposed CPABE and IBooS schemes is contrasted with the QP-BDHE system in this section. Because the storage of the vehicle and RSU is adequate, this differentiation define solely on the storage overhead of the cloud server. As a result, the vehicle and RSU may make efficient use of the storage.

Table 2. Storage Overhead of QP-BDHE, CPABE and IBooS

Algorithm	QP-BDHE	CPABE	IBooS
Storage overhead(bits)	5742	553	500

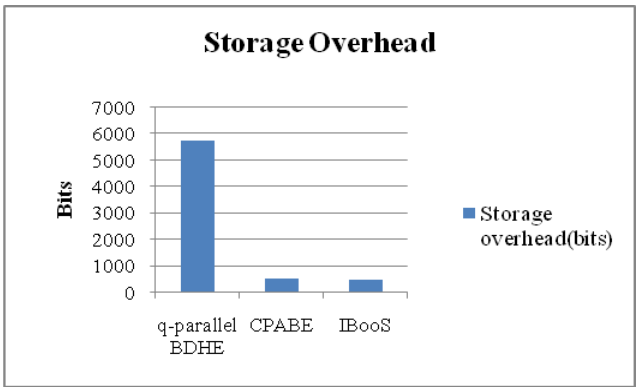

Fig. 5. Storage Overhead of QP-BDHE, CPABE and IBooS

The CPABE and IBooS scheme uses very little storage compared to the QP-BDHE scheme and as a result, it is idle for the vehicle data transmission with finite storage supplies.

C. Communication Overhead

In contrast to the q-parallel Bilinear Diffie Hellman Exponent scheme, the recipient in CPABE and IBooS schemes need the characteristics authority that aids in the decryption. However, the overhead of attribute revocation is considerably reduced since the attribute authority must upgrade any other's secret key in the QP-BDHE scheme, which is a significant overhead. To finish the attribute revocation non-impacting others in the organization, the attribute authority in CPABE and IBooS schemes can simply edit the element list of the one to be invalidated. As a result, CPABE and IBooS schemes clearly reduce total communication overhead.

Table 3. Communication Overhead of q-parallel BDHE, CPABE and IBooS

Algorithm	QP-BDHE	CPABE	IBooS
Communication overhead (bits)	49	5	6

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

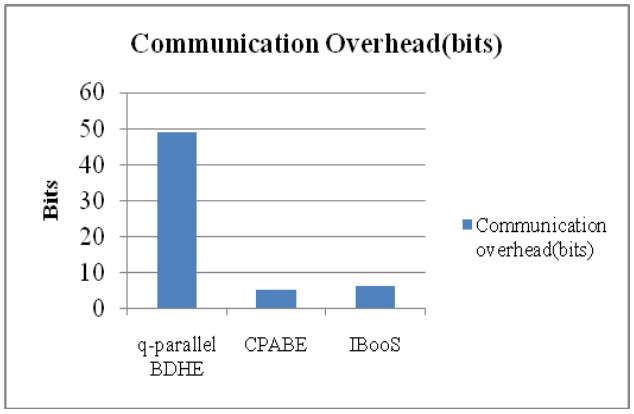

Fig. 6. Communication Overhead of q-parallel BDHE, CPABE and IBooS

The CPABE and IBooS scheme experience less communication overhead compared with the QP-BDHE scheme.

V. CONCLUSIONS AND FUTURE WORK

In the proposed work, an improved lightweight Vehicular Adhoc Network (VANET) architecture is designed to have efficient secure data transmission using effective data access control with Ciphertext Policy Attribute Based Encryption (CPABE). Also, Identity Based offline/online Signature (IBooS) is used to minimize the computation cost, storage overhead and communication overhead. The suggested method, based on the extensive security analysis and experimental assessment findings, not only protects user privacy but is also safe against different unwanted accesses. Moreover, the CPABE and IBooS scheme promises both scalability and efficiency. In future work, the scheme will be tested in a real world environment and calculate the communication latencies between entities. The Vehicular Ad-hoc Network can be implemented through the 5G devices and network utilizing edge computing.

REFERENCES

1. Huibin Xu, Mengjia Zeng, Wenjun Hu and Juan Wang, “Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs”, Hindawi Mobile Information Systems Volume 2019, Article ID 7016460, June 2019, www.hindawi.com.
2. Iftikhar Ahmad, Rafidah Md Noor, Muhammad Imran, Athanasios Vasilakos, Ihsan Ali, “Characterizing the Role of Vehicular Cloud Computing in Road Traffic Management”, International Journal of Distributed Sensor Networks, Vol. 13(5), 2017.
3. J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-Policy Attribute-Based Encryption.” In Proc. of SP’07, Washington, DC, USA, 2007.
4. Jian Shen, Tianqi Zhou, Jin Feng Lai, Pan Li and Sangman Moh, ”Secure and Efficient Data Sharing in Dynamic Vehicular Networks”, IEEE Internet of Things Journal, VOL. 14, NO. 8, August 2015.
5. John R. Vacca, “Cloud Computing Security Foundations and Challenges”, CRC Press Taylor & Francis Group”, 2017, ISBN 9781482260946.
6. Kai Hwang, Geoffrey C. Fox, Jack J. Dongarra, “Distributed and Cloud Computing From Parallel Processing to the Internet of Things”, *Morgan Kaufmann Publications*, Elsevier, 2013.
7. Kaigui Bian, Gaoxiang Zhang, and Lingyang Song, “Toward Secure Crowd Sensing in Vehicle-to-Everything Networks”, IEEE Network, 2018.
8. Mani Zarei, Amir Masoud Rahmani, “Analysis of Vehicular Mobility in a Dynamic Free-Flow Highway”, Elsevier Inc, 2016, https://daneshyari.com.
9. Marvy B. Mansour, Cherif Salama, Hoda K. Mohamed and Sherif A. Hammad, “VANET Security And Privacy – An Overview”, International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.2, March 2018, https://papers.ssrn.com.
10. Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, Rajkumar Buyya, “A survey on vehicular cloud computing”, Journal of Network and Computer Applications, www.citeseerx.ist.psu.edu.
11. Sheng Ding, Chen Li, and Hui Li, “A Novel Efficient Pairing-Free CP-ABE Based on Elliptic Curve Cryptography for IoT”, IEEE Access, Vol. 6, May 2018, https://ieeexplore.ieee.org.
12. Sonali P. Botkar, Sachin P. Godse, Parikshit N. Mahalle, Gitanjali R. Shinde, “VANET Challenges and Opportunities”, CRC Press Taylor & Francis Group. Boca Raton London New York, 2021.
13. Xiong Li, Tian Liu, Mohammad S. Obaidat, Fan Wu, Pandi Vijayakumar and Neeraj Kumar, “A Lightweight Privacy-Preserving Authentication Protocol for VANETs”, IEEE Systems Journal, May 2020.
14. Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, Zhenglin Liu. "A Privacy-preserving Trust Model based on Blockchain for VANETs", IEEE Access, 2018.
15. Jingwen Pan, Jie Cui, Lu Wei, Yan Xu and Hong Zhong, “Secure data sharing scheme for VANETs based on edge computing”, EURASIP Journal on Wireless Communications and Networking, June 2019.
16. Shi-Jinn Horng, Cheng-Chung Lu, Wanlei Zhou, "An Identity-Based and Revocable Data-Sharing Scheme in VANETs", IEEE Transactions on Vehicular Technology, 2020.
17. Yingying Yao, Xiaolin Chang, Jelena Misic, Vojislav B. Misic. "Lightweight and Privacy-Preserving ID-as-a-Service Provisioning in Vehicular Cloud Computing", IEEE Transactions on Vehicular Technology, 2020.
18. Kan Yang, Xiaohua Jia. "Attributed-Based Access Control for Multi-authority Systems in Cloud Storage", 2012 IEEE 32nd International Conference on Distributed Computing Systems, 2012.

AUTHORS PROFILE

Dr. J. Suguna, Ph.D., Associate Professor, Department of Computer Science, Vellalar College for Women, Erode – 638012, Tamil Nadu.

G. Keerthana, MCA., M.Phil., Research Scholar, Vellalar College for Women, Erode – 638012, Tamil Nadu.