

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/364083499>

Secure authentication and privacy-preserving to improve video streaming vehicle ad-hoc network

Article in Indonesian Journal of Electrical Engineering and Computer Science · October 2022

DOI: 10.11591/ijeecs.v28.i1.pp480-487

CITATIONS

0

READS

62

4 authors:



Akeel Kassim Leaby

University of Basrah

3 PUBLICATIONS 3 CITATIONS

[SEE PROFILE](#)



Mustafa Salah Khalefa

University of Basrah

36 PUBLICATIONS 91 CITATIONS

[SEE PROFILE](#)



Mushtaq A Hasson

University of Basrah

5 PUBLICATIONS 18 CITATIONS

[SEE PROFILE](#)



Ali adil Yassin

University of Basrah

97 PUBLICATIONS 596 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



COVID -19 + Information Technology + Scientific Research [View project](#)



Tacit Knowledge Sharing in Social Media [View project](#)

Secure authentication and privacy-preserving to improve video streaming vehicle ad-hoc network

Akeel Kassim Leaby, Mustafa Khalefa, Mushtaq A. Hasson, Ali A. Yassin

Department of Computer Science, Education College for Pure Science, University of Basrah, Iraq

Article Info

Article history:

Received Sep 19, 2021

Revised Jun 18, 2022

Accepted Jul 1, 2022

Keywords:

Ad Hoc

Authentication

Fully homomorphic encryption

Privacy

Vehicular ad hoc networks

Video summary

ABSTRACT

In vehicular ad hoc networks (VANET), the privacy of vehicle data symbolizes a big challenge towards malicious attacks. On the other side, vehicles in VANET can play a staple role in monitoring the environment by sensing the surrounding environment, compute the sensing information, and transfer the results if needed to the authorized party. Most of the modern VANETs systems encrypt the information to prevent hacking it but mostly neglect the decryption that occurred when data need to re-processed. In this paper, we try to cover this weak point by using fully homomorphic encryption (FHE) because of its specifications. The proposed work focus on twofold: first, create secure authentication and permission management system. While the second is to preserve the privacy of vehicle data that transferred among VANET infrastructure. This scheme also deals with metric security features, such as data privacy, data integrity, and key management. In the experimental results, there is good advance in the fields of interest comparing with the related works.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Akeel Kassim Leaby

Department of Computer Science, Education College for Pure Science, University of Basrah

Basrah 61004, Iraq

Email: akeel.kasim@uobasrah.edu.iq

1. INTRODUCTION

In a smart city environment, video streaming is one of the most promising applicable technologies [1]. By combining many technologies Vehicular ad hoc networks (VANETs) are expected to support mobility, reduce accident incidence, increase transport efficiency, and mitigate road risks [2], [3]. In VANETs, vehicles can send and receive video summary or multimedia entertainment through the VANET infrastructure [4]. This technique is used to improve road safety and passenger more comfortable. The general model of VANETs consists of three parts. In the first part there is a main processing center known as the trusted authority server (TAS) that is responsible for generating system parameters and subsequent permission. The second part, the road side units (RSUs), act as a router between vehicles and the TAS. All VANET vehicles contain sensor nodes used to sense the surrounding environment to provide relevant information to the TAS. Among the most critical types of information exchanged inside VANETs is vehicle data which exchanged between vehicles via vehicle-to-vehicle beacons (V2V) and between vehicles and system infrastructure over vehicle-to-infrastructures beacons (V2I) [5], [6]. The vehicle data includes biometric identity, vehicle location, traffic information and so on [7]. Because VANET protocols allow users to join and leave the network, a strong authentication scheme is also an important issue.

In some cases, the exchanged vehicle data needs to be processed or decrypted between VANET components [8]. This weakness can be infiltrated by attackers to obtain the exchanged information [9]. In this paper, the VANET model is compiled of four major elements: on-board unit (OBU), RSUs, TAS, and a video

monitoring system. In the Figure 1, we explain the main differences between traditional work and our contributes in this field depend on video summarization. So, Figure 1(a) illustrates a traditional VANET system, while Figure 1(b) outlines a VANET system supported by video streaming technology based on the proposed scheme. This model is support by visual monitoring systems installed inside RSUs and OBU to transmit information about the surrounding environment to the TAS. Each element carries out specific tasks such as identifying trespassers, registering vehicles which TAS recognizes, and defining system limits [10]. In our proposed scheme we choose fully homomorphic encryption (FHE) to secure vehicle and infrastructure data. FHE extends the scope of computations, providing the ability to process any data encrypted homomorphically [11]. The primary outline of this paper is as follows: section 2 provides details about basic tools and system models, the section 3 describes the proposed scheme, section 4 explains our experimental results and analysis and section 5 is the conclusion.

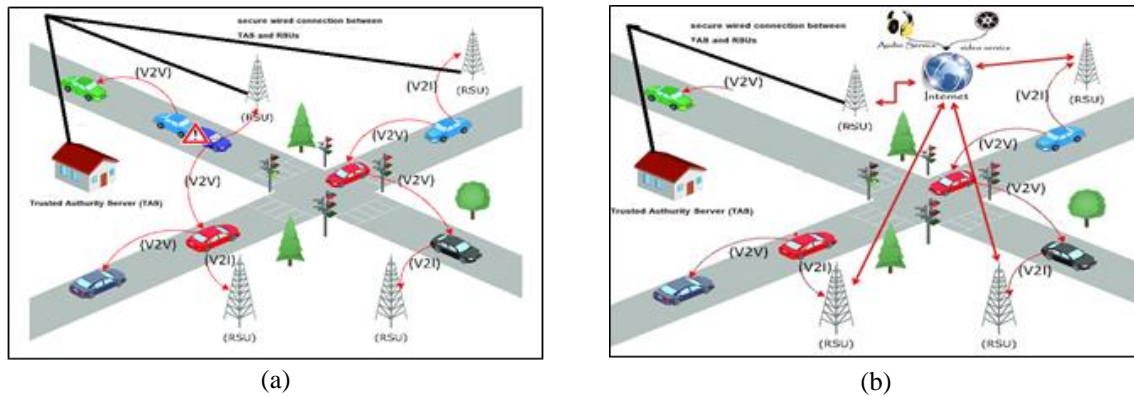


Figure 1. Denotes to main differences between traditional system and our work (a) traditional VANET system and (b) VANET system supported by video streaming

2. PRIMITIVES AND SYSTEM MODEL

2.1. Security and privacy requirements

To prove that our proposed scheme is safe and achieve reliable network, the following goals should be ensured in order to create secure authentication and permission management system:

- Message and video stream integrity and authentication. VANET ensures message and video stream integrity and the message and video stream beacons must check whether any content is corrupted during transmission.
- Privacy preservation: vehicles data should be secured.
- Traceability and revocation.
- Traceability and revocation: conditional anonymity should be offered to detect malicious vehicles and break their connection if necessary.
- Non-repudiation: senders of beacons and video streaming should forward receive data.
- Conditional anonymity: protect the normal vehicles real identity.
- Resistance to attacks: resisting attacks such as replay, impersonation, modification and MITM.

2.2. Cryptographic tool-(fully homomorphic encryption)

In 2009, Gentry [12] described FHE as a method allowing user to do calculations over encrypted data without need to decryption. As an important characteristics of FHE, the result of computations is also in an encrypted form [13]. FHE have become very important comparing with many another cryptographic tools [14]. In fact, FHE can be viewed as an extension for Symmetric-key or public-key cryptography [15]. Basically, let $(pn = K)$. Then if m_1, m_2, \dots, m_n are the cryptographic form of inputs. The encryption with multiplication of modulo K^2 . Then: the result also is on an encrypted form of $[m_1 + m_2 \text{ mod } K^2]$ this is because: $- ((1 + K)^{m_1} \cdot r_1^K) \cdot ((1 + K)^{m_2} \cdot r_2^K) = (1 + K)^{[m_1 + m_2 \text{ mod } K]} \cdot (r_1 \cdot r_2)^K \text{ mod } K^2$. Indeed, FHE has been widely used in consumer privacy in advertising, medical applications, data mining, financial privacy, and for forensic image recognition [16], [17].

2.3. System model

The proposed scheme can use in a VANET system with the following specifications: TAS should be fully trusted, generate all system parameters, can process any input information including video summary also can take the required decision, possess all component locations. RSU has the following ability: has built-

in camera device, can provide video streaming for surround environments or for received stream in real-time, deployed and collect VANET range, each neighbored RSUs interfered, finally all RSUs are connected and powered to each other and with TAS via secured wire system. OBUs: has a camera device, installed and powered inside vehicles, can send and receive from/to surround OBUs, and use IEEE 802.11p protocol to connect with other OBUs or with nearest RSUs.

3. RELATED WORKS

In this section, we offer an analysis of some previous works related to the authentication and privacy fields in VANET. We will focus on those protocols that are FHE based. Zhang *et al.* [15] proposed a secure communication and power injection scheme. This scheme can work over 5G grid slices and VANETs. The proposed scheme was collected from a trusted authority server, administration centre, power storage unit and roadside units. Additionally, the model contains several areas, such as parking and residential districts. Each of these areas contains a GetWay, which plays a role in communicating with the power storage units. Communication between a trusted authority server and GetWay uses a 5G slice grid. In this scheme, a trusted authority server decides the amount of power injected by power storage units. By applying both hash and then homomorphic technologies, the injected power is divided into time intervals and aggregated by each electrical vehicle.

In 2018, a secure task recomposition was proposed by Wang *et al.* [18]. This method is for computing in crowdsensing in VANETs fog. In this method, vehicles are assumed to have limited communication and computing capabilities. The cloud server acts as a services provider and a trusted authority center. All the system entities communicate with one another via dedicated short range communication 5G. The cloud server collects all results from subtasks. Based on these results, the cloud server recovers overall subtasks and tests reliability. The experimental results show an acceptable cost considering communication and computation.

In 2018, Ogundoyin [19] proposed a mechanism for traffic movement analysis. This mechanism is designed to ensure intelligent transportation system security. The traffic data (speed and data) collected from vehicles preserve privacy for all user information. Based on Chinese reminders and Paillier algorithms, the data aggregated, authentication bandwidth and time will be saved. In the proposed mechanism, the communication between trusted authority servers and vehicles relies on a secure channel. The trusted authority server will create a hash chain and generate a temporary private key. The transport management system analyses these aggregated data.

In 2019, Kong *et al.* [20] proposed a method to reduce the load on system resources. In the field of vehicles on the Internet, a secure data share scheme comprised roadside units, vehicles and traffic management systems. In this scheme, every vehicle builds its data report; then roadside units collect these reports from vehicles. After implementer the secure data aggregation, the aggregated data transferred to the traffic management system to take a decision.

Perma [21] proposed a modified fully homomorphic encryption scheme to reduce the computational cost by re-encrypt the data. This modified scheme required a communication cost less the required when using pillar schemes. The authentication technique is used to utilize data. This scheme uses mutual authentication technique to utilize data and access the server in VANETs. The experimental results show that it can prevent distance estimation errors and it is strong against malicious attacks.

In 2019, and based on fog computing, Sun *et al.* [14] proposed a stagy vehicles crowdsensing scheme used for data collection security. The proposed scheme is composed of fog buses, cloud data centers, upper-tier fog, data requester, and vehicles. A secure data aggregation based on the paillier algorithm and 2-DNF Formulas on Cipher texts [22]. The simulation evaluation metrics include the participation ration, successful participation ratio, and throughput. Simulation results show that it is suitable for the urban area of work.

In 2018, He *et al.* [23], designed a three steps ride-matching in ride-sharing scheme. The proposed scheme is implemented on some of NEXUS5 mobile phones. This scheme works under an Android 5 environment and uses Bluetooth 4 techniques. The experimental results show that it is efficient and secure to apply.

In 2019, Yucal *et al.* [24] suggest BMNNC method. This method uses peer-to-peer communications. The proposed method contains electrical vehicles and electrical power charging units. The vehicles firstly search for the nearest charging units, if there, then it will send a reply message in a reasonable time.

Ulybyshev [25] proposed a secure data exchanging scheme. The proposed scheme is based on access control attributions and rolls. The data exchange between any pairs of vehicles uses TCP/IP technique. The experimental results show that this method can prevent any data leakage caused by insider attacks. Table 1 shows a comparison between the related works on some sides.

Table 1. Comparison between related works

REF. /Year	Standard paillier computation	Data aggregation	Application scenario	Features
[15]- 2018	yes	Yes	Power injection scheme	Can the overall quantity of power only
[18]- 2018	yes	Yes	Task recomposition	Encrypt the sensed subtask at first
[19]- 2018	No	Yes	Analysis	Saving both bandwidth and authentication time
[20]- 2019	No	Yes	Data sharing	Save system resources
[21]- 2019	No	Yes	Data Aggregation	Keep distance estimation secure
[14]- 2019	Yes	No	Vehicle crowd sensing	Two- layers fog architecture
[23]- 2018	Yes	No	Ride-matching	Three steps
[24]- 2019	Yes	No	Online matching	Distributed scheme
[25]- 2018	Yes	No	Search	Supports the subset of query languages

4. PROPOSED SCHEME

The VANET was constructed from three major parts, TAS, RSU, and OBU. TAS is responsible and able to generates system parameters and manage all VANETs activities. While, OBE are connected to the nearest RSUs to transfer data between OBUs via V2V beacons or between OBUs and VANETs infrastructure via V2I beacons. Here, we note that there are two different types of connections, Ad-Hoc network and infrastructure. According to the third-party trust, OBUs may consider as fully reliable or not reliable for other operations. To prevent discreet communication in V2V beacons, OBU is used as a router. OBUs may contain several types of sensors such as cameras, radio, and heat sensors. All data recorded by these sensors are stored in internal storage inside vehicles until it is required to send it. The meaning of the frequently used notations that we used in our proposed scheme paper presented in Table 2. The main goal of this table is demonstrated the details of symbols in the proposed work.

Table 2. Preliminary notations

Preliminary notations	Symbols description
N	System parameter
G	Public system generator
R	Random number
cid	Computation identifier (public). The operation type is specified with cid
$H()$	Hash function
$L(*)$	Input bit length
N	Number of processing data
(sds, pds)	ds key pair
(sas, pas)	as key pair
$ds = pskds$	Public parameters of ds and as
(sj, pj)	de key pair (j)
(si, pi)	u key pair (i)
$[m]$	Cipher text of message
Mi	Raw data from de, i
$[m] +$	Re-encryption of message m by ds
$m \frac{1}{2} _pi$	Ciphertext of message m under pi

4.1. Computational tools

VANETs services or beacon services (BS) which provides correlation of OBUs in the Ad-Hoc network of VANET. To compute the security of V2I beacons, an access sensor is used. When data is encrypted and collected; data encrypts (DE) is used for other computational analysis also. Vehicles OBUs (VO) process and deals with encrypted data. Table 2 shows all preliminary notations we used in the proposed scheme. In this research, the aim to ensure the safe beacons transmission inside VANET with or without deployment. Beacons include much critical information such as speed, location, and identity. In our work, we propose a scheme focus on beacons privacy preservation when it encrypted or decrypted. Also, TAS generates, update, and revoke all vehicles that joined to VANET. The generated pseudonym of any vehicle is given by $ps = \text{time}||p(\text{rid})|| \text{hc}||\text{RSU}$. Where: ps is the pseudonym generated by TAS, p(rid) represents the value of the real vehicles identity after encryption using public key pk and vehicles home code hc. In the proposed scheme, the information are broadcasted from RSU towards OBUs periodically. The following steps illustrates the proposed scheme, (V2V beacons authentication, vehicles in range of home authentication with RSU, RSU pseudonym generation and broadcasting, V2I authentication, cross V2V authentication, and authentication inside software).

4.2. Setup function

Let: ds follow paillier cryptosystem. When it encrypt similar keys p will represented as $(m_i)_p$ where $(i = 1,2,3 \dots Q)$. Where $D_s(T1_{i=1}^Q [m_i]) = \sum_{i=1}^Q m_i$. Let r,t as large prime numbers where $n = \text{mul}(r, t)$. So, let G is group cycle element, G,g,and h represent maximal order elements. Then $h =$

$g^x \bmod n^2$ where $x \in [1, \alpha(n^2)]$ and $\alpha(0)$ is the Euler function with x as co-prime factor. Hence, the additive homomorphic encryption [12], [13].

$$D_s(T1_{i=1}^Q [m_i]) = \sum_{i=1}^Q m_i \tag{1}$$

4.3. Key encryption function

In this section h, g and n represents a parameters has a secure value α . In the subsection 4.1, we illustrate the major jobs and distributes keys used in encryption/ decryption exchanged messages between components in VANET’s environment. The following steps refers to encryption function.

- Generate $h = g^x \bmod n^2$ where $x \in [1, \alpha(n^2)]$.
- Cipher key generation is done by using:

$$\{m\}_n = (T, T) = (h^r(1 + m^o n), g^x) \bmod n^2 \tag{2}$$

- By knowing both h and m values, then the decryption is done by using:

$$m = Q\left(\frac{T}{T^x}\right) \bmod n^2 \text{ where } Q(u) = \left(u - \frac{1}{n}\right) \tag{3}$$

4.4. Key decryption function

There are two parameters used to generate a key. This key is used to secure message. These parameters are security and large primary numbers (p, q) sequentially:

$$L(p) = k = L(q), \quad p = p + 2p, \quad q = 1 + 2q, \quad n = pq$$

$$\text{So, } p = P_{bs}^{sk_{as}} = P_{as}^{sk_{bs}} = g^{ab} \bmod n^2 \tag{4}$$

The p is used as a public key for all users. The p will broadcast to all vehicles for using in encryption/ decryption to exchange data between components. The Table 3 illustrates the resulted equations. In this scheme, we note from Table 2 equations that there is an impact for both secret key length and data length. The following sections discuss these influence in details.

Table 3. Equations of operations

Operation	Equation
Generation of cipher text of two key encryption (2KE)	$(w_i) = (w_i)_p = (T_i, T_i')$ (5)
	Where $T_i = (1 + w_i n) P^r \bmod n^2$ and $T_i' = g^r \bmod n^2$, $r \in (1, 0.25n)$ and $m_i \in z_n$ and $P = server$
Decryption of two keys (2KD)	$(w_i)_{p^{ac}} = [(1 + w_i n)_{p^{ac}} p^r g^{ra}] \bmod n^2$ (6)
	Where:- $T_i^{/(2)} = P^r \bmod n^2$, $w_i = L\left(\frac{T_i}{T_i^{/(2)}}\right) \bmod n^2$
Initial re-encryption (IRE)	$h_2 = L_1[(P_j)^{sac} \parallel c_{rid}]$, $(w_i)_{p_j} = [T, T]$ $= (T, (T')^{sac} g^{h_2})$ (7)

4.5. Impact of secret key length (bits)

The length of the secret key (in bits) is the estimated re-encryption method. The secret key length can be taken between (150-300) bits by increasing 25 bits for each step. To get the required results, the network density is increased. As shown in Table 4 and Figure 2, the relationship between the estimated cost with the length of the secret key.

Table 4. Influence of secret key length

Secret key length	Enc	Dec	2KE	2KD	IRE	RDEn
175	6.3	10	4.3	16	7	15.9
200	10	10.513	4.8	16.3	7.3	15.8
225	13.2	13	5	20	9	16.3
250	20.3	20	5.8	22	12.5	15.3
275	23.2	22.8	7.89	16.7	18	16.3
300	23.8	24	10.33	15.3	24.5	16.4

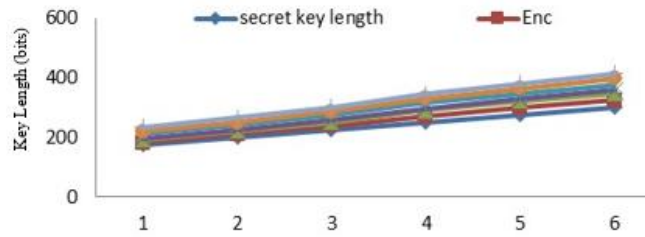


Figure 1. Influence of secret key length

4.6. Impact of input data length (bits)

In this scheme, we note all the transferred information is sending or receive as (beacons). In the experimental test, we try different beacons lengths. We start from (50-300) bits in 25 bits step. Table 5 explained the resulted from changing different beacons lengths. From the resulted values, we note that the proposed scheme can deals with different sizes of beacons since it does not apply any compression method. Since the data we used in the proposed system model are mainly multimedia, we note that an increase in overhead with increase the beacon size. Figure 3 show the resulted values curve for all steps.

Table 5. Influence of input data length (bit)

Input data length	Enc	Dec	2KE	2KD	IRE	RDEn
50	14	5.9	12.1	5	12.6	14.9
75	14.1	6	12.1	6	12.6	14.9
100	14.7	6.1	12.3	6.1	12.6	14.9
125	14.8	6.18	12.3	6.4	12.6	14.8
150	14.9	6.2	12.3	6.3	12.6	14.7
175	15	6.38	12.4	6.4	12.7	14.6
200	15.2	6.4	12.5	6.4	12.7	14.6
225	15.2	6.4	12.5	6.4	13	14.5
250	15.3	6.55	12.5	6.4	12.7	14.5
275	15.4	6.6	12.6	6.4	13	14.5
300	15.5	6.7	12.7	6.4	13.1	14.45
325	15.5	6.7	12.7	6.45	13.2	14.34
350	15.7	6.8	12.8	6.45	13.2	14.22
375	15.8	7	12.9	6.45	14	14.2

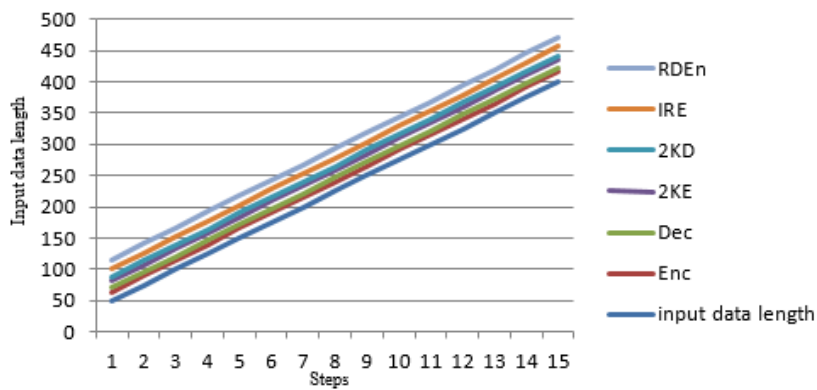


Figure 2. Influence of input data length (bit)

5. CONCLUSION

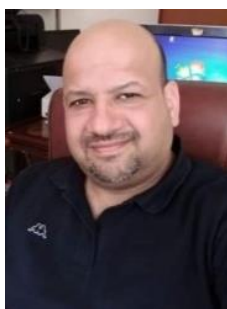
We proposed privacy preservation scheme using FHE in VANET, so the beacons will encrypted when send and till received. The FHE scheme will transfer insecure manner via VANETs components. Our work scheme protects the beacons with a high level of security. Also, the proposed scheme reduces the compression time, which leads to an increase in the system model overhead with long secret keys and with long beacons. In VANET construction, mutual authentication is provided using both ds and as. A dual authorized entry also





gives the proposed scheme a special feature. We conclude from experimental results that the impact of both security key and beacon on system performance and overhead.

REFERENCES





- [1] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: a systematic review," *Sustainable Cities and Society*, vol. 55, p. 102023, 2020, doi: 10.1016/j.scs.2020.102023.
- [2] M. Elhoseny and K. Shankar, "Energy efficient optimal routing for communication in VANETs via clustering model," in *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks*, ed: Springer, 2020, pp. 1-14, doi: 10.1007/978-3-030-22773-9_1.
- [3] R. Karthick, "Development of secure transport system using VANET," *Test Eng. Manag.*, vol. 82, no. 13, pp. 2073-2078, 2020.
- [4] S. More and U. Naik, "Optimal multipath routing for video transmission in VANETs," *Wireless Personal Communications*, pp. 1-23, 2020, doi: 10.1007/s11277-020-07740-1.
- [5] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja, and K. S. Kumar, "Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography," in *Cybersecurity and secure information systems*, ed: Springer, 2019, pp. 193-204, doi: 10.1007/978-3-030-16837-7_9.
- [6] Z. Lin and Y. Tang, "Distributed multi-channel MAC protocol for VANET: An adaptive frame structure scheme," *IEEE Access*, vol. 7, pp. 12868-12878, 2019, doi: 10.1109/ACCESS.2019.2892820.
- [7] A. Srivastava, A. Prakash, and R. Tripathi, "Location based routing protocols in VANET: Issues and existing solutions," *Vehicular Communications*, vol. 23, p. 100231, 2020, doi: 10.1016/j.vehcom.2020.100231.
- [8] A. M'tumbe, "Analysis of data exchange of vehicle-to-vehicle communication in VANET," *HNURE*, 2020.
- [9] O. S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, and A. Rachedi, "UAV-assisted supporting services connectivity in urban VANETs," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 3944-3951, 2019, doi: 10.1109/TVT.2019.2898477.
- [10] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Information Sciences*, vol. 476, pp. 211-221, 2019, doi: 10.1016/j.ins.2018.10.021.
- [11] S. Carpov *et al.*, "Privacy-preserving semi-parallel logistic regression training with fully homomorphic encryption," *BMC Medical Genomics*, vol. 13, pp. 1-10, 2020, doi: 10.1186/s12920-020-0723-0.
- [12] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme* vol. 20: Stanford university Stanford, 2009.
- [13] F. Armknecht *et al.* "A guide to fully homomorphic encryption," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1192, 2015.
- [14] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *Journal of Network and Computer Applications*, vol. 134, pp. 89-99, 2019, doi: 10.1016/j.jnca.2019.02.018.
- [15] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50-60, 2018, doi: 10.1016/j.jnca.2018.07.017.
- [16] M. Mina-Zicu and E. Simion, "Threats to modern cryptography: grover's algorithm," 2020, *Preprints*: 2020090677.
- [17] B. Yu, W. Mao, Y. Lv, C. Zhang, and Y. Xie, "A survey on federated learning in data mining," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 12, p. e1443, 2022, doi: 10.1002/widm.1443.
- [18] B. Wang, Z. Chang, Z. Zhou, and T. Ristaniemi, "Reliable and privacy-preserving task recomposition for crowdsensing in vehicular fog computing," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1-6, doi: 10.1109/VTCSpring.2018.8417688.
- [19] S. O. Ogundoyin, "An anonymous and privacy-preserving scheme for efficient traffic movement analysis in intelligent transportation system," *Security and Privacy*, vol. 1, p. e50, 2018, doi: 10.1002/spy2.50.
- [20] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644-655, 2019, doi: 10.1016/j.future.2017.12.003.
- [21] N. Prema, "Efficient secure aggregation in VANETs using fully homomorphic encryption (FHE)," *Mobile Networks and Applications*, vol. 24, pp. 434-442, 2019, doi: 10.1007/s11036-018-1095-y.
- [22] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of cryptography conference*, 2005, pp. 325-341.
- [23] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 5994-6005, 2018, doi: 10.1109/TVT.2018.2809039.
- [24] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019, doi: 10.1016/j.adhoc.2018.07.029.
- [25] D. Ulybyshev, A. O. Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. B. Othmane, "Secure data communication in autonomous v2x systems," in *2018 IEEE International Congress on Internet of Things (ICIOT)*, 2018, pp. 156-163, doi: 10.1109/ICIOT.2018.00029.

BIOGRAPHIES OF AUTHORS







Asst. Lecturer Akeel Qasim Leaby     is an lecturer in Department of computer science, college of pure science, University of Basrah, Basrah, Iraq, since 2015. He received his Master degree from computer science department, Sudan University, Sudan. He hold his Bachelor degree from Department of computer engineer, Kirkuk university, Kirkuk, Iraq from 2002 to 2006. He can be contacted at email: akeel797@gmail.com.







Prof. Dr. Ali A. Yassin     is a Professor with the Department of Computer Science, College of Education for Pure Science, University of Basrah. He received the bachelor's and master's degrees from the University of Basrah, Basrah, Iraq, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China. His research interests include the security of cloud computing, image processing, pattern recognition, biometrics, data integrity, DNA cryptography, steganography, sharing data, graphical password, QR code, and soft computing. He can be contacted at email: alihak@upm.edu.my or ali.yassin@uobasrah.edu.iq.



Dr. Mustafa S. Khalefa     received the Science degree in Computer Science from University of Basrah in 2005, and the Aggregation in Computer Science, Software Engineering from University Technology Malaysia (UTM) from Malaysia, Rabat, in 2009. He received the Master degree in Software engineering from Faculty of Computer Science and Technology; in 2017 he completed His Ph.D. in Information System and Software Engineering from University Putra Malaysia from faculty of Computer Science and Information Technology department of Information system and Software Engineering. Mustafa Currently work as lecturer and researcher for University of Basra, Faculty of Pure Science, Computer Science department, in addition he is consultant for many companies and training center with many skills in top management, currently research interest are in: Software Engineering, Information System, Information Technology, Ontology, Knowledge Management, Enterprise resources Planning, Internet of Things, Business analysis and business development, Globule virtual team, leadership. Where he is the author for Many research publication. He can be contacted at email: mustafakhalefa@gmail.com.



Mushtaq A. Hasson     is an lecturer in Department of computer science, University of Basrah, Iraq, since 2013. He received his Master degree from computer science department, Huazhong university of Science and Technology, Hubei, wuhan, China, from 2010 to 2012. The Topic of his master dissertation was in the field of data mining (Ranking Algorithm). The current research interest are in Software engineer, data mining, web classification, cloud computing and blockchain. He hold his Bachelor degree from Department of computer science, University of Basra, Iraq, from 2004 to 2007. He can be contacted at email: mushtaq.husson@uobasrah.edu.iq.