

Received February 29, 2020, accepted March 18, 2020, date of publication March 30, 2020, date of current version April 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982636

# Efficient Privacy-Preserving Scheme for Location Based Services in VANET System

FIFI FAROUK<sup>1</sup>, YASMIN ALKADY<sup>2</sup>, AND RAWYA RIZK<sup>1</sup>

<sup>1</sup>Technology and Information Systems Department, Port Said University, Port Said 42526, Egypt

<sup>2</sup>Electrical Engineering Department, Port Said University, Port Said 42526, Egypt

Corresponding author: Rawya Rizk (r.rizk@eng.psu.edu.eg)


**ABSTRACT** A Vehicular Ad-hoc Network (VANET) is a type of Mobile Ad-hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. VANET is not only used for road safety and driving comfort but also for infotainment. Communication messages in VANET can be used to locate and track vehicles. Tracking can be beneficial for vehicle navigation using Location Based Services (LBS). However, it can lead to threats on location privacy of vehicle users; since it can profile them and track their physical location. Therefore, to successfully deploy LBS, user's privacy is one of major challenges that must be addressed. In this paper, we propose Privacy-Preserving Fully Homomorphic Encryption over Advanced Encryption Standard (P<sup>2</sup>FHE-AES) scheme for LBS query. This scheme is required for location privacy protection to encourage drivers to use this service without any risk of being pursued. It is implemented using Network Simulator (NS-2), Simulation of Urban Mobility (SUMO), and Cloud simulation (CloudSim). Analysis and evaluation results demonstrate that P<sup>2</sup>FHE-AES scheme can preserve the privacy of the drivers' future routes in an efficient and secure way. The results prove the feasibility and efficiency of P<sup>2</sup>FHE-AES scheme in terms of query's response time, query accuracy, throughput and query overhead.

**INDEX TERMS** Advanced encryption standard, CloudSim, fully homomorphic encryption, LBS, MANET, NS-2, privacy-preserving, SUMO, VANET.

## I. INTRODUCTION

Nowadays, significant time and gas are wasted every day as a result of traffic congestion and slow traffic. The large scale and frequent usage of vehicles has given rise to the pressing need for Location Based Services (LBS). Responsible governments are paying much attention to better manage traffic by investing in new technologies like Global Positioning System (GPS) [1], Traffic Management Center (TMC) [2] and vehicular ad hoc network (VANET) [3].

GPS-based navigation systems become popular. In such a system, a small hardware device is installed on a vehicle. By receiving GPS signals, the device can determine its current location and then find the geographically shortest route to a certain destination based on a local map database. However, the route searching procedure of these systems is based only on a local map database, and real-time road conditions are not taken into account.

The associate editor coordinating the review of this manuscript and approving it for publication was Weisi Guo .

TMC is used for real-time road conditions, which has been adopted in a number of developed countries. TMC makes use of Frequency Modulation (FM) radio data system to broadcast real-time traffic and weather information to drivers. Special equipment is required to decode or to filter the information received. However, only special road conditions (e.g., severe traffic accident) are broadcasted and a driver cannot obtain information like the general fluency of a road from TMC.

Recently, VANET becomes increasingly popular in many countries. It is an important element of the Intelligent Transportation Systems (ITSs) [4]. In VANET, each vehicle is assumed to have many entities. An On-Board Unit (OBU) is located on the top of the vehicle itself to allow a vehicle to communicate with other vehicles and with the infrastructure, Road-Side Units (RSUs) is installed along the roads, a Registration authority (RA) is used to provide authentication and authorization services to the vehicles. LBS provider (LBSP) and maybe some other application servers are installed in the back end. The OBUs and RSUs communicate using

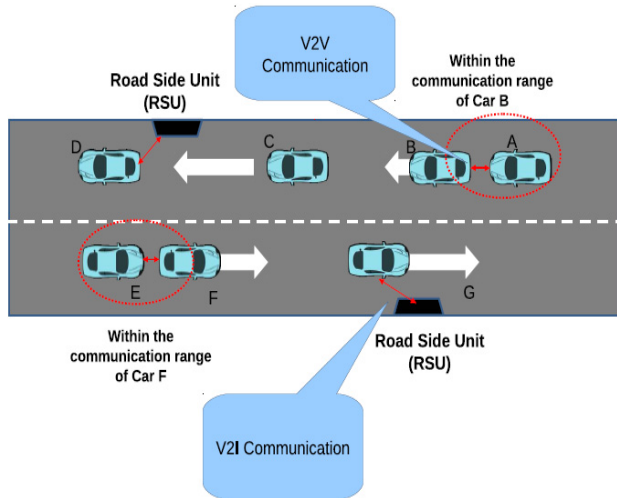


FIGURE 1. VANET communication system.

the Dedicated Short-Range Communications (DSRC) protocol [5] over the wireless channel while the RSUs, RA, and the application servers communicate using a secure fixed network (e.g., the Internet).

VANET communication can be divided into two categories: Vehicle-to-Infrastructure (V2I) communication, and Vehicle-to-Vehicle (V2V) communication as shown in Figure 1. The first type happens between the vehicle and the infrastructure deployed on the roads, referred as RSUs, which communicate with nearby vehicles. V2V communication is typically used for broadcast safety messages like pre-collision warning, electronic road signs, traffic light violation warning, online vehicle diagnosis, and road condition detection from vehicles to other nearby vehicles [6].

The VANET enables useful functions such as cooperative driving; probing vehicle data that increases vehicular safety, reducing traffic congestion, and offering access to LBS. LBS provides many applications. For example, a vehicle requests the nearest neighbor such as the nearest restaurant, hotel, or supermarket. Obviously, search services facilitate driving. Nevertheless, in order to obtain the exact result, a vehicle always offers a real location to the LBSP. In addition, LBSP will provide services taking into consideration information about the vehicle, like its speed and the license plate number in order to answer the vehicle's request effectively.

However, mapping the physical location of the vehicle with that of the user can violate the location privacy of the user and reveal his identity. With the fact that vehicular networks are open where everyone can sniff what is transmitted, comes a great concern over how to protect the user's privacy [7].

Therefore, in this paper we propose Privacy-Preserving Fully Homomorphic Encryption over Advanced Encryption Standard (P<sup>2</sup>FHE-AES) scheme for LBS query. It is based on improving Fully Homomorphic Encryption (FHE) over Advanced Encryption Standard (AES) to avoid noise concatenating with encrypted message; which results when using FHE alone. This noise results in lack of efficiency due to severe communication overhead problem.

In P<sup>2</sup>FHE-AES scheme, the LBSP's data are outsourced to the cloud server in an encrypted manner, and a registered vehicle user can get accurate LBS query results without divulging his/her location information to the LBSP, RSU or the cloud server.

The rest of the paper is organized as follows. Section II introduces the problem statement. Section III covers the related work. Section IV presents the preliminaries. Section V covers the system model, adversary model considered, and proposed system. Section VI describes security analysis. Section VII evaluates the performance of the proposed scheme. Section VIII concludes our work and discusses the future work.

## II. PROBLEM STATEMENT

In this section, we address the avoidance of unauthorized location tracking of vehicles, and the alleviation of profiling of LBSs accessed from the LBSP by vehicles. The location tracking of any vehicle leads to the following vulnerabilities:

### A. MISUSED LOCATION INFORMATION OF VEHICLES

The location information of vehicles can be misused for crimes, such as abductions or automobile thefts. It presents threats to the location privacy of the vehicle user [8].

### B. PROFILING OF PERSONAL INTERESTS OF THE VEHICLE USER

The location tracking of any vehicle includes locations that have been visited. Therefore, location history of the vehicle user can be accumulated over time and the visited locations of the vehicle can be associated with places of interest (POIs), thereby enabling inference and profiling of personal interests of the vehicle user [9]. It presents threats to the location privacy.

### C. RSU PRESENTS THREATS

RSUs are not trusted and curious. Since they are placed along roadside, they can be easily compromised. Also, they are curious about drivers' privacy such as navigation queries. It presents threats to the location privacy of the vehicle user.

### D. LBSP UNTRUSTED ENTITY

LBSP needs to know critical personal information about the vehicle user such as his location and Identity (ID). In order to deliver the intended service; which is finding information such as nearby restaurants, fuel stations and touristic places. Thus, the LBSP, which is untrusted entity, can profile the user and his interests, pinpoint his location and track him leading to his destination. Due to their privacy threats, vehicle users would prefer not to use this service offered from the VANET system. By this, insuring a location privacy protection scheme will promote the use of such services.

Therefore, in this paper we propose P<sup>2</sup>FHE-AES scheme to ensure the privacy of users' vehicles while using LBS in VANET system. This scheme relies on FHE over AES cryptography. The message or query will be secured by encrypting

it with AES then the encrypted data will be evaluated homomorphically with FHE.

### III. RELATED WORK

Location privacy for users' vehicles in VANET has been actively researched over the past years. Many of the envisioned proposed schemes for hiding user's location and identity are presented as follows:

#### A. K-ANONYMITY

K-Anonymity [10] is a typical location privacy-preserving method for LBS. It proposes the concept of forming k-anonymous region. The location is sent in the name of a group of k users and not by the user himself. By this, his precise location will not be identified. However, this concept makes users dependent since the user should wait for k other users in order to send his request. This scheme cannot be applied in low user density areas. Moreover, because a user will have to wait until at least k users are present in his vicinity in order to submit his request, the waiting time may lead to delays which degrade the quality of the service in terms of the user's location in time and in space, and hence cannot be applied to real-time services. K-Anonymity scheme requires a trusted third party (TTP). However, the TTP is easy to become a performance bottleneck. Once the TTP compromises, all privacy will be leaked because the TTP knows all the real locations.

#### B. PSEUDONYMS UPDATING

E. C. PSEUDO [11] introduced the concept of using temporary identities named as pseudonyms which are not related neither to the vehicle identification number nor to the driver identity. Users update their pseudonyms for each location request at crossroad which will confuse attackers about the real identity of the sender of the request. However, this method does not always help in location privacy since some applications need a long-term communication relationship so changing pseudonyms may interrupt this communication which is complex to be reestablished.

When RSUs distribute pseudonyms to vehicles, the amount of traffic in the network increases. This increase may lead to reduction of the bandwidth essential for other applications.

#### C. COMMUNICATIONGROUP LEADER AGENT (CGLA)

AMOEBAs [12] and LPA [13] presented the group concept to provide anonymous access to LBSs where only one node, denoted as Group Leader (GL), communicates with the LBS on behalf of the other group members concealing by this the source of the request. A vehicle sends messages through a GL anonymously. The GL is not only responsible for forwarding messages, but also for signature, verification, encryption, and decryption. It is easy to become a bottleneck. Nevertheless, GL may have left the group before a server responds, due to rapid movement of a vehicle, and thus the group communication is difficult to maintain. This technique relies on a single

GL that presents a single point-of-failure for group members to access services.

#### D. HOMOMORPHIC APPROACH

Due to the capacities such as confidentiality, integrity, and authenticity, homomorphic primitives are taken as desirable building blocks to realize position privacy. For the sake of concealing the real identity of a user, POSTER [14] and TK-FHE [15] are used to answer queries without learning or revealing any information of the query. Meanwhile, since the computational result of ciphertext matches that of the plaintext, homomorphic cryptosystems are also valued as promising tools for location privacy application. Homomorphic approaches are adopted to resist active attacks. These schemes require more exponential computation and produce high overhead due to the noise associated with the ciphertext.

In summary, all the above schemes suffer from major privacy infringements that enable attackers to profile participating users by sniffing into the network, knowing the user's identity and following them knowing their destinations. In P<sup>2</sup>FHE-AES proposed scheme, we address solutions for the mentioned drawbacks as will be evident next in Section V.

### IV. PRELIMINARIES

In this section, some preliminaries are introduced that we build P<sup>2</sup>FHE-AES scheme upon including FHE and AES properties

#### A. SECURE MULTIPARTY COMPUTATION

Secure multiparty computation (SMC) was first proposed in Yao's Millionaires problem [16] where, the secure multiparty computation property has been applied in the distance verification. In P<sup>2</sup>FHE-AES scheme, it is assumed that there are  $n$  vehicle nodes, namely  $\{V_1, V_2, \dots, V_n\}$ , wanting to compute a function  $f$  with some secret inputs held locally by some of the vehicle nodes. The function  $f$  is typically specified as:  $(\{0, 1\})^{*n} \rightarrow (\{0, 1\})^*$ . The vehicle  $V_i$  has input  $x_i \in \{0, 1\}^*$  and output  $y_i \in \{0, 1\}^*$ , where  $(y_1, \dots, y_n) = f(x_1, \dots, x_n)$ .

It means that these vehicle nodes can compute correct outputs collectively, and any individual vehicle node  $V_i$  doesn't know any information about the inputs and outputs of the other vehicles than itself [17].

#### B. OVERVIEW OF AES

The AES algorithm is a symmetric encryption algorithm that operates on 128-bit data blocks supporting three different key sizes of 128, 192, and 256 bits. The P<sup>2</sup>FHE-AES scheme referred to use AES-128. An AES encryption process consists of a number of encryption rounds that depends on the size of the key. The standard calls for AES-128 is 10 rounds. The round function operates on a  $4 \times 4$  matrix of bytes. The basic operations that are performed during the round function are *AddKey*, *SubBytes*, *ShiftRows*, and *MixColumns* [18], [19]. Each AES operation is examined in turn, and how it is implemented homomorphically is described in [20]. The proposed P<sup>2</sup>FHE-AES scheme chose to shoot for an evaluation of AES.

Since it seems like a natural benchmark, AES is widely deployed and used extensively in security-aware applications (so it is “practically relevant” to implement it). Moreover, the AES circuit has a regular (and quite “algebraic”) structure, which is amenable to parallelism and optimizations. Indeed, for these same reasons, AES is often used as a benchmark for implementations of protocols for SMC, for example [21]–[23].

**C. HOMOMORPHIC ENCRYPTION DEFINITION**

In abstract algebra, a homomorphism is a structure-preserving map between two algebraic structures, such as groups. Where a group  $G$  combines two elements  $a$  and  $b$  to form another element, denoted  $a \oplus b$ . To qualify as a group, the set and operation,  $(G, \oplus)$  must satisfy four requirements known as the group axioms:

1) CLOSURE

For all  $a$  and  $b$  in  $G$ , the result of the operation,  $a \oplus b$ , is also in  $G$ .

2) ASSOCIATIVITY

Is given by (1) For all  $a, b$ , and  $c$  in  $G$

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) \tag{1}$$

3) IDENTITY ELEMENT

For every element  $a$  in  $G$ ,  $G$  contains at most one identity element  $e$  that satisfies the given (2)

$$e \oplus a = a \oplus e = a \tag{2}$$

4) INVERSE ELEMENT

For each element  $a$  in  $G$ , there exists an inverse element  $a^{-1} \in G$  and  $e$  is identity element, the inverse element satisfies (3)

$$a \oplus a^{-1} = a^{-1} \oplus a = e \tag{3}$$

The identity element of a group  $G$  is often written as 1 in multiplicative identity and written as 0 in additive identity. The result of an operation may depend on the order of the operands. In other words, the result of combining element  $a$  with element  $b$  need not yield the same result as combining element  $b$  with element  $a$ ; (4) may not always be true.

$$a \oplus b = b \oplus a \tag{4}$$

This equation always holds in the group of integers under addition, because (5) shows that:

$$a + b = b + a \tag{5}$$

Given two groups  $(G, \otimes)$  and  $(H, \oplus)$ , a group homomorphism from  $(G, \otimes)$  to  $(H, \oplus)$  is a function  $f : G \rightarrow H$  such that for all  $g$  and  $g'$  in  $G$  as shown in (6)

$$f(g \otimes g') = f(g) \oplus f(g') \tag{6}$$

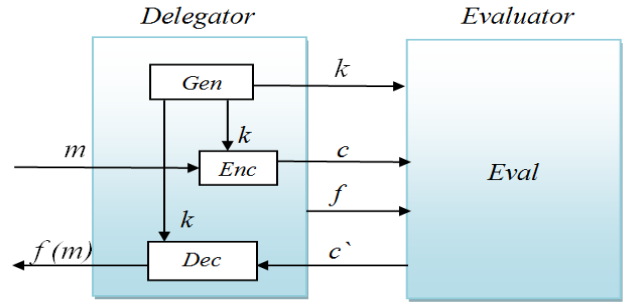


FIGURE 2. FHE over AES symmetric key.

Let  $(P, C, K, E, D)$  be an encryption scheme, where  $P$  and  $C$  are the plaintext and ciphertext spaces,  $K$  is the key space, and  $E$  and  $D$  are the encryption and decryption algorithms, respectively. Assume that the plaintexts forms a group  $(P, \otimes)$  and the ciphertexts forms a group  $(C, \oplus)$ , then the encryption algorithm  $E$  is a map from the group  $P$  to the group  $C$ , i.e.,  $E_k : P \rightarrow C$ , where  $k \in K$  is either a secret key (in a secret key cryptosystem) or a public key (in a public-key cryptosystem). For all  $a$  and  $b$  in  $P$  and  $k$  in  $K$ , as shown in (7).

$$E_k(a) \oplus E_k(b) = E_k(a \otimes b) \tag{7}$$

**D. FHE OVER AES**

FHE-AES is based on matrix operations which are computationally “light”. It uses symmetric keys of small size thereby making it suitable for many data centric applications. It derives its security from hardness of factorizing a large integer [24], which is basis of many public key cryptosystems.

As shown in Figure 2, FHE over AES scheme is used to design an efficient and practically feasible FHE that uses AES symmetric algorithm [20]. It can handle arbitrary size of computations without the need of noise management and has scope of parallelization [24], [25]. AES presents a good design space to investigate FHE techniques because it supports parallel nature of computation and algebraic nature of computation.

The basic concept is to translate operations on integers in a ring  $M_4(\mathbb{Z}_n^*)$ ;  $M_4$  means that all operations are on square matrices of size 4, and  $\mathbb{Z}_n^*$  means a set of integer numbers in algebra theory, and  $M_4(\mathbb{Z}_n^*)$  are sufficiently small to be used practically.

FHE over AES is used to optimize communication with the cloud without bootstrapping [26]. In the context of making a FHE scheme to be useful enough, we proposed a scheme with following set of operations: *KeyGen*, *Enc*, *Eval* and *Dec* which are explained in details in [20].

**V. SYSTEM MODEL**

In our system model, we mainly focus on how LBSP offers accurate and efficient service to users’ vehicles based on VANET system and satisfy privacy-preserving location data.

**A. VANET SYSTEM MODEL**

VANET system is a vehicular communication systems contain many entities.

### 1) VEHICLES

Vehicles communicate with each other and with road side units (RSUs) that are spread along the road. They are able to store cryptographic credentials and running cryptographic algorithms. Additionally, vehicles are equipped with GPS receivers to know its current location. Vehicles use the location information to determine whether the segments inquired by RSUs are in its route.

### 2) ON-BOARD UNIT (OBU)

An OBU allows vehicle to communicate with other vehicles and with the infrastructure [27]. This unit is placed on the top of the vehicle itself.

### 3) ROAD SIDE UNIT (RSU)

A RSU is one of the main components of the infrastructure through which vehicles communicate with application servers. RSUs are access points that receive the encrypted routes from passing vehicles and act as a relay to the Traffic Management Center (TMC). They are connected to the TMC via fast communication technology, e.g., wired cables, 4G, or WiMax. RSUs are located aside the roads and are interconnected via a wired network.

### 4) REGISTRATION AUTHORITIES (RA)

RA provides authentication and authorization services to both vehicles and LBSP.

### 5) TRAFFIC MANAGEMENT CENTER (TMC)

Each TMC is responsible for monitoring the traffic in a number of segments. It is connected to the group of RSUs that covers the segments of interest. It can also receive traffic information from other TMCs. After processing the traffic information, it sends recommendations to the vehicles to avoid slow and congested road segments. Additionally, TMC can control the traffic lights in its segments to facilitate the traffic movement. For example, they can prolong the green light on busy roads [28].

### 6) LOCATION BASED SERVICE PROVIDER (LBSP)

LBSP records all the location data forwarded by the RSUs, and processes the data together with information from other data sources for example, vehicle manufacturers and TMC.

### 7) CLOUD SERVER PROVIDER (CSP)

Encrypted LBS query request submitted by a legal user to LBSP which outsources large-scale location data to the cloud server to be managed by CSP for enjoying the low-cost storage services and powerful computation services. CSP is responsible for computing the shortest way to the desired destination. In the whole query processes, the CSP does not know any contents about outsourced location data, the user's query request, and the current location of the LBS user.

Figure 3 illustrates Vehicles move on roads, sharing collective environmental information between themselves, and with

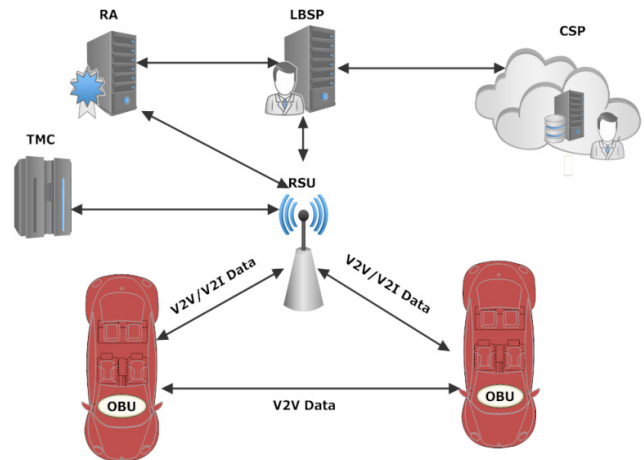


FIGURE 3. VANET system model.

the servers via RSUs. In this environment, units or entities can be interconnected permanently. Inside this environment mainly contains the entities that manage traffic and also gives access to external services.

A vehicle is enabled with an OBU for V2V and V2I communications, and sensors (for example, GPS) and database units to collect environmental information (for example, vehicle location, vehicle speed, and tire pressure).

RSUs connected to LBS which provides an interface for LBSP. In addition, RA provides authentication and authorization services to both vehicles and LBSP.

## B. SECURITY THREATS

### 1) ATTACK ON PRIVACY

Privacy preservation is so significant for vehicles that the related personal sensitive information, including driver's name, license plate, speed, location, and traveling routes, has to be protected to some extent. Privacy attack can be in these forms:

- Identity revealing: The process of authentication might reveal a driver's private information through their vehicles.
- Location tracking: The location or path is also a part of the personal privacy data of a vehicle, which should not be used improperly or be leaked.

### 2) FREQUENCY ANALYSIS THREAT

Since CSP and LBSP are able to track and record access frequencies, then they may infer some locations by analyzing the access pattern. For example, a user tends to visit home and work more often compared to other places.

### 3) ATTACK ON CONFIDENTIALITY

As an important security property, confidentiality can avoid messages to be altered in the storage and transmission processes. Once the confidentiality has been violated, the adversary might launch an attack to change the source or content of those messages and utilize them to escape from the forensics.

#### 4) ATTACK ON IDENTIFICATION AUTHENTICATION

Identification authentication is an essential part to provide secure communications in VANETs. In order to guarantee secure and reliable delivery, the sender should not be able to tamper the message and the receiver can verify it, no matter where it comes from. There are mainly two kinds of approaches for identifying and authenticating; including impersonation attack and sybil attack. In impersonation attack, the adversary pretends to be another party in the communication. This attack can be done by stealing pseudonym and identity (ID)based keys of others. In sybil attack, the adversary illegitimately claims multiple identities to communicate with RA and RSU at the same time. Since wireless channels are broadcast in nature, this attack will likely result in more serious damage.

#### C. PROPOSED SYSTEM

Some important hints are taken into consideration:

- The TMC divides the roads into segments and gives a unique identifier for each segment. The identifier can be derived from the segment coordinates and the road name.
- The TMC preloads each RSU with its nearby segments. Each RSU is responsible for querying the passing vehicles.
- The RA is always online. RSUs and RA communicate through a secure fixed network. To avoid being a single point of failure or a bottleneck, redundant RAs which have identical functionalities and databases are installed. The RSU to vehicle communication (V2I) range is at least twice that of the inter-vehicle communication (V2V) range to ensure that if a RSU receives a message, all vehicles receiving the same message are in the feasible range to receive the notification from the RSU.
- The real identity of any vehicle is only known by the RA, TMC and the vehicle itself, and is saved on OBU but not by others. Each vehicle generates pseudo identity PID to communicate with LBSP through corresponding RSU.
- In proposed scheme, we assume that LBSP is already authorized by RA.

In this section, the proposed privacy-preserving scheme P<sup>2</sup>FHE-AES is described in details. Table 1 shows the notations used in the system. The proposed scheme consists of six basic phases, System Initialization, Registration, Data Creation, Revocation, Query Verification, and Location Data Encryption and Decryption. These phases are shown in Figure 4 and described as follows:

##### 1) SYSTEM INITIALIZATION

RA generates a unique public parameter  $\lambda$  for each vehicle and publishes the public generator parameter  $g$  for LBSP.

First, the  $VU_i$  receives  $\lambda$  as input from corresponding RSU, then running  $keyGen(\lambda)$  to compute  $SK$  to encrypt its message or query. The key arranged in the form of a matrix of  $4 \times 4$  bytes in  $Z_n^*$ , hence does not involve any

TABLE 1. List of notations.

Symbol	Definition
$\lambda$	security parameter
$AS_i$	Attribute- Set
$ASP$	Access Structure Policy
$C_d$	Destination category
$D_d$	Description of destination
$DEC_{AES}$	AES decryption function
$ENC_{AES}$	AES encryption function
$Eval$	Evaluation function of fully homomorphic
$g$	Generator parameter
$H$	Hashing function using MD5
$keyGen$	Key generation function
$KList$	List of registration keys
$Lat$	Value of Latitude in Radians
$long$	Value of Longitude in Radians
$M_4$	matrix of size 4
$MD5$	Message Digest Algorithm 5
$pi$	Value of $Pi$ is 22/7
$PID$	Pseudo Identification
$POI$	Place of Interest
$regK_i$	Registration-Key
$SK$	Secret Key of AES
$T_d$	Destination title
$VU_i$	Vehicle User, $i$ refer to the user number
$X_d, Y_d$	Destination coordination
$X_i, Y_i$	Current user coordination
$Z_n^*$	Denote the set of all integers

computation theoretically.  $keyGen(\lambda)$  is described in key generation function.

```

/* Key generation Function */
Keygen(){
  int  $\lambda$ ;
  /*  $\lambda$  is a security parameter */
  1. Pick a matrix  $k$  of size 4,  $k \in M_4(Z_n^*)$ ;
  2.  $SK = Keygen_{AES}(\lambda)$ ;
  3. output ( $SK$ ); }

```

In addition,  $VU_i$  also implements AES symmetric encryption algorithm  $Enc_{AES}$  before sending query.  $VU_i$  selects a random value  $X \in Z_n^*$  to perform a secure cryptographic MD5 hashing function  $H$  in the system, where  $H: \{0, 1\}^* \rightarrow Z_n^*$  maps a message of arbitrary length to an element in  $Z_n^*$  to check integrity [29].

From discrete assumption problem there is cyclic group  $G$  which generates the parameter of bilinear group called  $g$  [30]. The mapping  $\hat{e}: G \times G \rightarrow G_T$  is called a bilinear map if it satisfies the following properties:

- Bilinear:  $\forall P, Q, R \in G$  and  $\forall A, B \in Z_n^*$ ,
  - $\hat{e}(Q, P + R) = \hat{e}(P + R, Q) = \hat{e}(P, R) = \hat{e}(R, Q)$
  - Also  $\hat{e}(aP, bP) = \hat{e}(P, bP)^a = \hat{e}(aP, P)^b = \hat{e}(P, P)^{ab}$
- Non-degenerate: There exists  $P, Q \in G$  such that  $\hat{e}(P, Q) \neq 1$ .

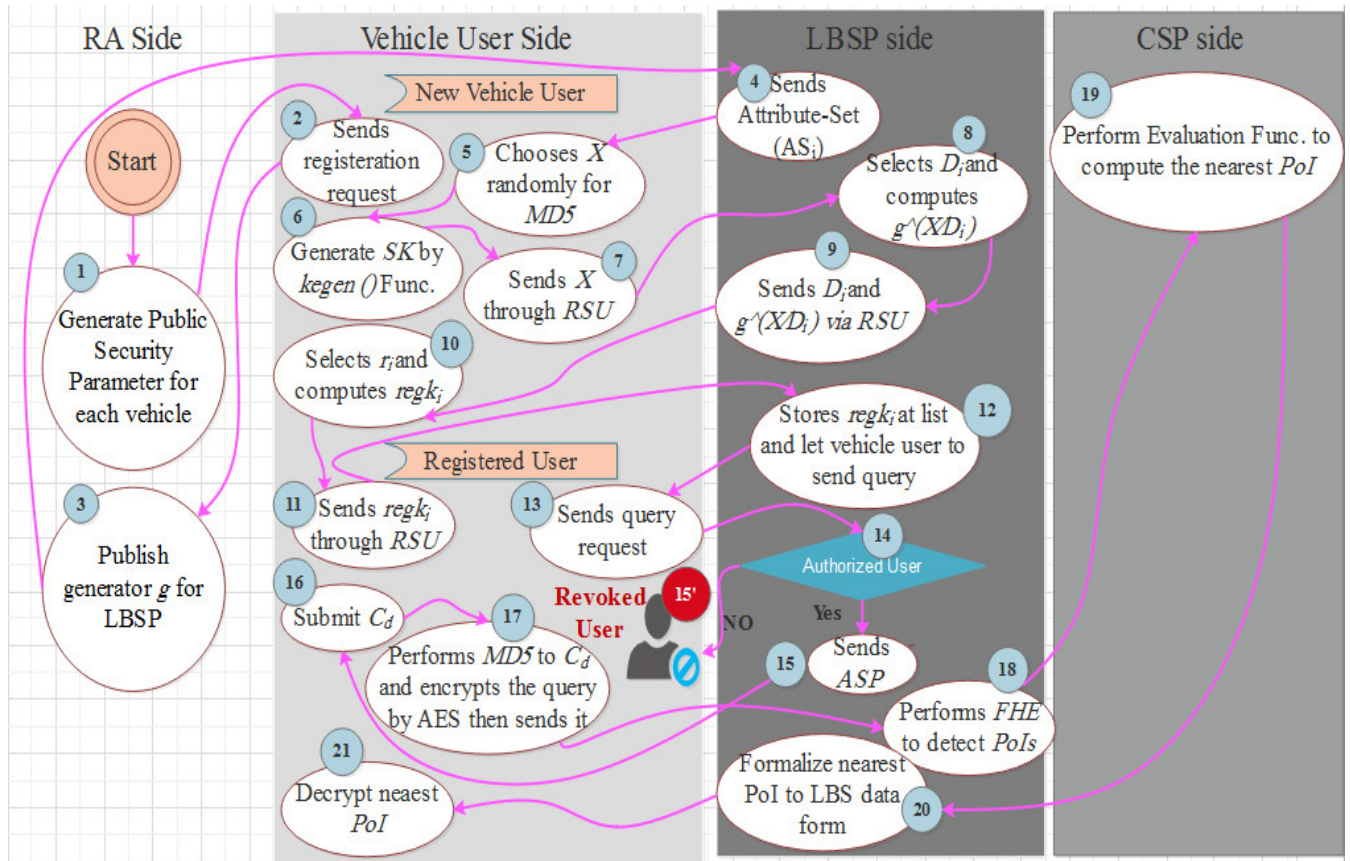


FIGURE 4. P<sup>2</sup>FHE-AES phases.

- Computable: There exists an efficient algorithm to compute  $\hat{e}(P, Q)$  for any  $P, Q \in G$ .

$VU_i$  keeps  $\langle SK, X \rangle$  as the master key secretly then sends  $\langle X \rangle$  to LBSP through RSU via secure channel. LBSP selects a random value  $D_i \in Z_n^*$  and computes  $g^{X/D_i}$ . Then LBSP sends  $\langle g^{X/D_i}, D_i \rangle$  to  $VU_i$  through RSU via secure channel.

## 2) SYSTEM REGISTRATION OF NEW VEHICLE USER

The proposed system considered that LBSP is already registered in VANET system. So that LBSP is authorized in VANET system by RA.

The  $VU_i$  needs to register to use LBS in order to get service and send queries, the  $VU_i$  gets the data field *Attribute-Set* ( $AS_i$ ) from the LBSP through RSU and randomly selects  $r_i \in Z_n^*$ . Then  $regK_i$  is computed as:

$$regK_i = g^{X/D_i} \times g^{r_i} \quad (8)$$

$VU_i$  sends  $regK_i$  to LBSP through RSU via secure channel and stored in LBSP at *KList*. As a registered  $VU_i$  of the LBSP,  $VU_i$  is authorized with  $\langle regK_i \rangle$  which will be utilized for retrieving LBS resources in a privacy-preserving way later. During the registration,  $VU_i$  negotiates permissions to get access to groups of data records and *ASP*. *ASP* is

generated by LBSP. It is used to determine whether the  $VU_i$  has permissions to access a record.

At the end of registration process,  $VU_i$  sends  $regK_i$  to the LBSP through RSU via the same secure channel as a registration request. Then LBSP verifies that  $regK_i$  is the element of *KList*. After that, LBSP selects *ASP* based on the input of  $AS_i$  represented by  $regK_i$ ; which is described in the following authentication function.

```

/* Authentication Function */
Authenticate(){
    1. int regKi;
    2. list KList;
    /* klist is a list of keys that saved on LBSP */
    3. if ( regKi ∈ KList)
    /* verifying regKi is the element of KList */
    4. then VUi ← ASP (regKi);
    /* Selecting ASP according to detected user */
    5. Else
    Return("Not Authenticated");}
    
```

## 3) SYSTEM DATA CREATION

In general, the LBSP has plenty of LBS resources, and most of resources' information. The LBS data construction is organized as a category set and a location data set. A CATEGORY

denotes the general name of location data sets. Each location data set is a four-tuple  $\{PID, T_d, (X_d, Y_d), D_d\}$  where  $d$  indicates destination location and belongs to  $C_d$  in a category set. All these attributes describe the detailed information of a certain location as shown in the following example:

Category Set {CATEGORY}	Location Data Set {PID, TITLE, COORDINATE, DESCRIPTION}
Hotel: {	{250, Huatian Hotel, (x <sub>250</sub> , y <sub>250</sub> ), (5 stars)},
	{251, Westin Hotel, (x <sub>251</sub> , y <sub>251</sub> ), (4 stars)},
	...
	{500, Four Seasons Hotel, (x <sub>500</sub> , y <sub>500</sub> ), (5 stars)}

In this paper, the query size is assumed 30KB, and FHE is adopted over AES to encrypt LBS data. The proposed scheme allows the LBSP to provide totally the same query service over encrypted location data as the plaintext environment aforementioned; i.e. if information about the location data and user’s query request is exposed to LBSP.

In P<sup>2</sup>FHE-AES scheme,  $VU_i$  needs to encrypt the interested CATEGORY by hashing function MD5. Then the location coordinates are encrypted by AES, which are sent by  $VU_i$  to LBSP through RSU. Thus, RSU and LBSP have  $VU_i$ ’s data that they can’t expose.

LBSP performs FHE over AES encrypted data. CSP performs computations on outsourced encrypted data according to proposed scheme. Of course, the necessary decryption operations need to be involved for  $VU_i$  once receiving the encrypted LBS query result through RSU.

#### 4) VEHICLE USER REVOCATION

User revocation is an essential yet challenging task in practical application such as LBS system. In this scheme, an efficient user revocation mechanism is proposed while being able to effectively prevent the revoked  $VU_i$  from having the service. More concretely, for a  $VU_i$  who will be revoked by LBSP, the LBSP scans the user information in the  $KList$  to find out the information of  $VU_i$  and deletes  $(VU_i, regK_i)$ . Once  $(VU_i, regK_i)$  is deleted from  $KList$ ,  $VU_i$  no longer has the capability to get a response to his request and search location data because this user is already revoked as shown in Figure 5.

If a  $VU_i$  is revoked for three consecutive times, LBSP will send a spam report to TMC through corresponding RSU. This report is a complaint about revoked  $VU_i$  attempts to LBS system. Then TMC takes action against revoked  $VU_i$ . The spam report is described at the following function.

```

/* Spam Report to TMC */
Spam_Report( ){
    1. Input: reg Ki, KList;
       //klist and regKi are global variables.

```

```

2. For(int count = 0;count < 3;count++)
3. {
4. Get(regKi);
5. if( regKi ∈ KList)
6. {
7. Return ("Authorization User");
8. Break;
9. }
10. Else {
11. Return ("Not_Authorization_User");
12. Continue;}
13. }
14. if(count == 3)
15. Return ("SpamReport");
16. }

```

#### 5) QUERY VERIFICATION

In P<sup>2</sup>FHE-AES scheme, the request verification is very important step using MD5 as shown in (9) to increase the sample space of location information; this can resist the exhaustive attack. It is shown in the following function.

$$E_1 = H(PID, C_d)^X \tag{9}$$

```

/* Query Verification */
Q_verify(){
    1. String PID; /* PID is Pseudo item */
    2. String Cd; /* Cd is category item */
    3. int X;
       /* X is a secret value generated by user and sends
       to LBSP */
    4. E1 = H(PID, Cd)X;
    5. if(E1 is a valid Hashing Function)
    6. {Return (Accept) }
    7. Else
    8. {Return (Reject)}
    9. }

```

#### 6) QUERY ENCRYPTION AND DECRYPTION

Generally, after query verification when  $VU_i$  searches a location of interest,  $VU_i$  submits the specified  $C_d$ , his/her current location coordinates, and destination location coordinates which is determined by GPS [1].

This process is implemented at vehicle user side and at LBSP side as follows:

##### a: IMPLEMENTING AES AT VEHICLE USER SIDE

To achieve the security of location data, the  $VU_i$  needs to encrypt all location information with AES before sending it to LBSP through RSU. LBSP needs to perform FHE over AES encrypted data before outsourcing them to the CSP which is responsible for detecting the nearest location. Outsourcing encrypted data saves computation time at LBSP.



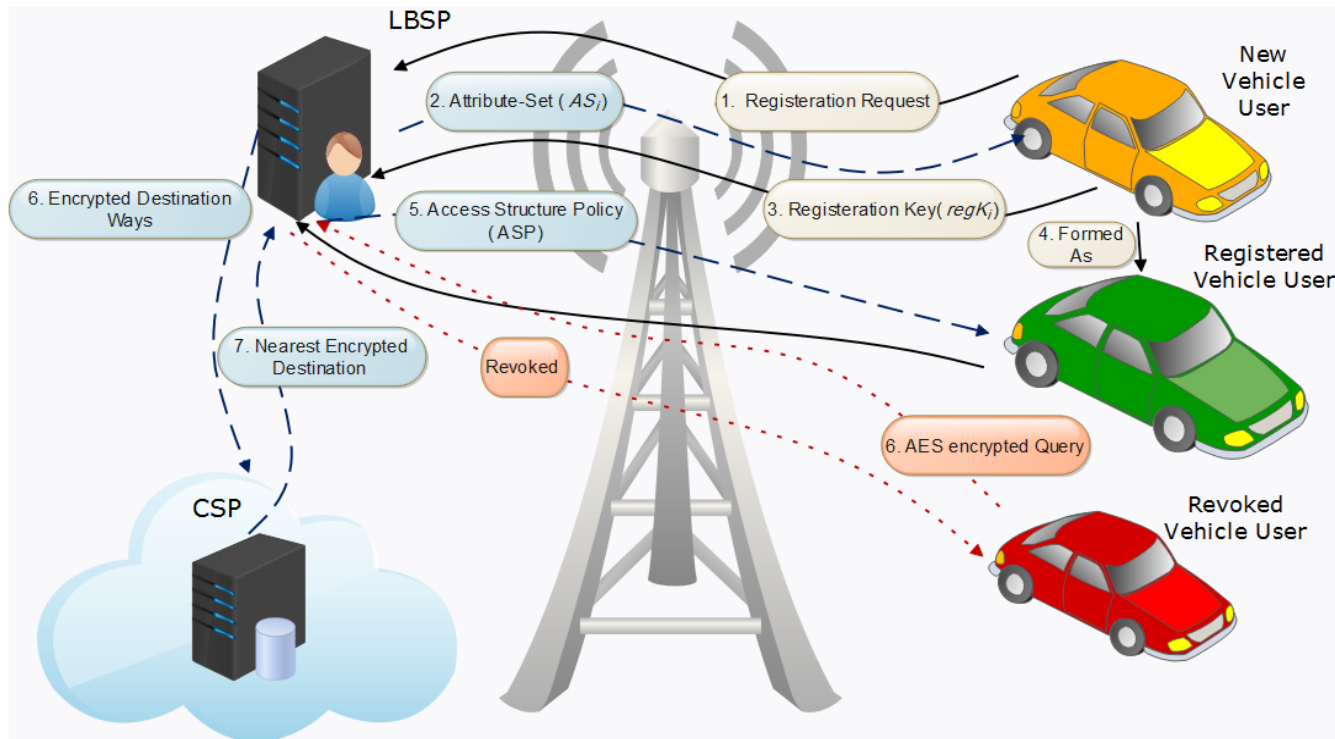


FIGURE 5. System registration.

To enable an efficient privacy-preserving LBS query, P<sup>2</sup>FHE-AES scheme will be used to encrypt the different attributes of the location data. It takes the following steps to encrypt the location data sets:

First,  $VU_i$  adopts AES symmetric Encryption scheme to encrypt *TITLE* and *DESCRIPTION* attributes. It can be implicitly formed by:

$$E_2 = ENC_{AES}(T_d, D_d, SK) \quad (10)$$

Second,  $VU_i$  uses the secretly preserved invertible matrix  $M_4$  to encrypt destination coordinates  $(X_d, Y_d)$ . It can be implicitly formed by:

$$E_3 = ENC_{AES}(M_4(X_d, Y_d), SK) \quad (11)$$

Third,  $VU_i$  adopts AES symmetric Encryption scheme to encrypt current location coordinates  $(X_i, Y_i)$  arranged in the form of a matrix  $M_4$ ; it can be formed by:

$$E_4 = ENC_{AES}(M_4(X_i, Y_i), SK) \quad (12)$$

For the output encrypting collection; that is encrypted query  $EQ_1$ . It can be implicitly formed by:

$$EQ_1 = \{E_2, E_3, E_4\} \quad (13)$$

*b: IMPLEMENTING FHE AT LBSP SIDE*

To preserve  $VU_i$ 's query privacy as well as to enable correct search, and detecting nearest destination over encrypted

location data, LBSP performs fully homomorphic evaluation function over AES encrypted data. There is a general evaluation function *Eval* defined to perform basic operations *f* (addition, subtraction, multiplication and division) on encrypted data  $EQ_1$  as illustrate in (14). The importance of evaluation function in LBSP is to detect all the ways leading to required destination which refer to required POIs.

$$EQ_2 = Eval(f, EQ_1) \quad (14)$$

These two functions are described as follows:

```

/* Encryption at vehicle user side */
Enc_User(){
1.  $E_2 = ENC_{AES}(T_d, D_d, SK)$ ;
/* Performing AES Encryption function to
TITLE and DESCRIPTION attributes */
2.  $E_3 = ENC_{AES}(M_4(X_d, Y_d), SK)$ ;
/* Performing AES Encryption function to Coordination of destination attribute */
3.  $E_4 = ENC_{AES}(M_4(X_i, Y_i), SK)$ ;
/* Performing AES Encryption function to Coordination of user */
4. output ( $EQ_1 = \{E_2, E_3, E_4\}$ );
5. }
/* Concatenates result in form of Encrypted Query and sends it to LBSP */
    
```

```

/* Evaluation function at LBSP side */
Eval_LBSP(EQ1){
1.  $E_2' = Eval(f, E_2)$ ;
2.  $E_3' = Eval(f, E_3)$ ;
3.  $E_4' = Eval(f, E_4)$ ;
4.  $List\_EQ2 = \{E_2', E_3', E_4'\}$ ;
5. output ( $List\_EQ2$ );

```

Then LBSP sends  $List\_EQ2$  of the ways leading to specific destination to CSP to achieve privacy-preserving. The powerful CSP searches over encrypted outsourced location data on behalf of the user query. CSP returns encrypted target location (closest POIs to the user location) and sends it to LBSP.

The distance between target location  $T$  and  $VU$  is calculated using *haversine* formula [31]; it is also known as great circle distance. It is one of the example methods that use for resolve distance calculation problem and this method is also used for many researches. *Haversine* formula is the method that is used to calculate distance between two coordinates on two-dimensional map. The distance is the actual distance by which the earth's spherical trigonometry. This formula performs calculation from main point to destination point with trigonometric function by using latitude and longitude. In the calculation steps *haversine* is first will change the value of the latitude and longitude integer number into radians by dividing them by  $180/\pi$ ; It can be implicitly formed by (15-16). The value of  $180/\pi$  is approximately 57.29577951.

$$lat = Latitude/(180/\pi) \tag{15}$$

$$long = Longitude/(180/\pi) \tag{16}$$

Then these numbers are calculated in the algorithm *haversine*. The formula of *haversine* is:

$$d = 3963.0 * \cos[(\sin(lat\ VU) * \sin(lat\ T)) + \cos(lat\ VU) * \cos(lat\ T) * \cos(long\ T - long\ VU)] \tag{17}$$

where  $d$  is the distance between the two coordinates on two-dimensional map. It is measured by miles. It can be measured by kilometers by multiplying  $d$  by 1.609344.

Then CSP selects the closest POI by the following function and sends it to LBSP who translates into LBS data form and sends the result attached with hashing value  $E_1$  to  $VU$ .

```

/* Minimum POI formalization at LBSP side */
Formal_Q( ) {
1-  $EQ3 = Q(\text{closest POI})$ ;
/*  $Q$  is a function that puts closest POI in a query form */
2- Output ( $EQ3$ );
3- }

```

Finally,  $VU_i$  performs decryption process described in the following decryption function.

```

/* Decryption function at user side */
Dec_User(E1, EQ3){
1.  $(PID, C_d)^X = decode(E_1)$ ;
/* decode is tools to decrypt MD5 by comparing hashed value with database */
2.  $(T_d, D_d) = DEC_{AES}(E_2')$ ;
/* Performing AES Decryption func. to return TITLE and DESCRIPTION attributes */
3.  $(X_d, Y_d) = DEC_{AES}(E_3')$ ;
/* Performing AES Decryption func. to destination Coordination attribute */
4.  $(X_i, Y_i) = DEC_{AES}(E_4')$ ;
5. }
/* Performing AES Decryption func. to user Coordination attribute */

```

## VI. SECURITY ANALYSIS

In this section, the security properties of P<sup>2</sup>FHE-AES scheme are analyzed. Specifically, following the problem statement discussed earlier, the analysis will focus on how the proposed scheme in VANET system can achieve the security.

### A. PREVENTING CONFIDENTIALITY ATTACK

Confidentiality cannot be violated in P<sup>2</sup>FHE-AES scheme. Because P<sup>2</sup>FHE-AES scheme avoids messages to be altered in the transmission processes by using MD5 hashing function to check the data integrity after transmission processes. Therefore, the proposed P<sup>2</sup>FHE-AES scheme guarantees secure and reliable query delivery by checking data integrity. Moreover; the LBSP and CSP cannot expose the origin query content. The confidentiality is achieved when LBSP obtains encrypted data with a secure symmetric AES algorithm, and also P<sup>2</sup>FHE-AES scheme can achieve confidential LBS data. Specifically, the cloud sever cannot obtain the actual location information of the resource; although it can get all the outsourced data items and users' query information, but these outsourced data are in encrypted form). In P<sup>2</sup>FHE-AES scheme, before the LBSP publishes its encrypted data items to the CSP, each item is evaluated homomorphically by using FHE over AES.

### B. PREVENTING AUTHENTICATION ATTACK

P<sup>2</sup>FHE-AES scheme achieve authentication; because each registered  $VU$  is signed by secure mechanism with the help of ASP to make the source authentication guaranteed. Moreover, for any unregistered  $VU$ , since he/she does not have the secret  $regK_i$ , he/she also cannot submit valid query request to the LBSP.

Even if the impersonation attack occurred, the data will be safe by using P<sup>2</sup>-FHE-AES scheme because the data is encrypted by symmetric AES algorithms and only true  $VU$  is able to decrypt this data (which is the only one who knows  $SK$ ).

### C. PREVENTING LOCATION TRACKING AND IDENTITY REVEALING

Partial information from the LBS server is leaked; in this case, an attacker can obtain partial information from the LBS server. The data will be safe by using P<sup>2</sup>FHE-AES scheme because the data is encrypted by symmetric AES algorithms before uploading the data to the LBS server. After that, the encrypted data is evaluated homomorphically to perform computation without divulging the origin query information. In this way, even if the data on the LBS server are leaked, attackers still cannot restore the raw data because only *VU* knows the secret key to decrypt the encrypted data. Since RSU, LBSP, and CSP deal with users' data in encrypted form only, they cannot track the location, and thus the attacker cannot use any of them to perform location tracking.

There is no ability for attackers to succeed in identity revealing, because the real identity of *VU* is only known by the RA, TMC and the vehicle itself, and it is saved on OBU but not by others. Each vehicle generates pseudo identity; to communicate with LBSP through corresponding RSU. So that, the identity attached in query is not the real identity, it's just a pseudo identity. Moreover; the query is already encrypted.

### D. PREVENTING FREQUENCY ANALYSIS ATTACK

CSP and LBSP cannot be able to track and record access frequencies. The proposed P<sup>2</sup>FHE-AES scheme prevents the curious behavior of CSP and LBSP to know any private information belonging to *VU* and his query, because CSP and LBSP deal with the users' data in encrypted form.

## VII. PERFORMANCE EVALUATION

### A. SIMULATION TOOLS

In this section, the performance of P<sup>2</sup>FHE-AES scheme is evaluated from the perspective of *VU*, LBSP, and CSP. The software and hardware configurations of *VU*<sub>*i*</sub> and LBSP side are performed on a 64-bit Ubuntu 12.04 LTS system with an Intel Core i7 processor and 32GB RAM. The CSP side is a virtual machine with Intel Xeon processor E5-4600, 64 GB memory on the Dell blade server M830, and VMware vSphere ESXi OS. The open source Charm library [32] is applied to implement the pairing group operations, which is supported by the standard PBC library [33] and FLINT [34] is applied for the finite field arithmetic in  $Z_n^*$ . We used Github library [35]; this library is written in C++ and uses the NTL mathematical library for obtaining the C++ source code and we adopted the FHE over AES scheme released in HELib. A real-life dataset OpenStreetMap [36] is used which contains 62556 real world locations.

### 1) NETWORK SIMULATION

The NS-2(version-2.35) tool [37] was used to conduct the simulations in the proposed system since it is the most widely used network simulator.

### 2) TRAFFIC SIMULATION

Beside network simulation, a well-designed traffic simulation is also essential to successfully simulate the proposed system. There are many traffic simulators as CORSIM, Bonn-Motion, Vissim, VanetMobiSim, and Simulation of Urban Mobility SUMO [38].

SUMO is used for traffic mobility simulation of the proposed P<sup>2</sup>FHE-AES scheme. SUMO can show the road traffic in microscopic view that can be used to develop road topology with its vehicle, road, junction, and traffic light built with parameters to define vehicles traffic direction and speed.

We extended available NS-2 satellite models to obtain specific instrument for P<sup>2</sup>FHE-AES scheme simulation. Every time the request from *VU* and response from LBSP has to route to CSP. This model can easily be simulated in NS-2 taking LBSP as the routing point. At this router, we assume some amount of time delay for authentication activity which is performed with every request. Also some fraction of the processing time (at LBSP) is devoted to obfuscation or any other anonymity technique to make the user anonymous.

### 3) CLOUD SIMULATION

CloudSim is used for P<sup>2</sup>FHE-AES [39]. It is a toolkit supports modeling of cloud environment under single or multiple clouds. It supports number of cloud system components like data centers, virtual machines, and resource provisioning policies.

## B. PERFORMANCE METRICS

Performance metrics are an essential scale by which we can compare between different schemes: *K-anonymity* [10], *E.C.PSEUDO* [11], *AMOEB*A [12], *LPA* [13], *POSTER* [14], *TK-FHE* [15], and the proposed P<sup>2</sup>FHE-AES.

In our simulations, we assume a communication channel supported by an IEEE 802.11. There are total 10 to 500 vehicles moving along the roads in a random walk away with max speed 120 km/hour where a real map based on Ismailia city, Egypt scenario has been used. The query size is fixed 30 Kbytes. In each vehicle, the movement model is Map-Route-Movement.

The evaluation parameters include both privacy efficiency and communication efficiency parameters in order to prove that the proposed scheme can achieve privacy efficiency without any effect on communication efficiency.

### 1) PRIVACY-PRESERVING SCHEMES

As shown in Table 2, the comparison between privacy-preserving schemes in terms of Query Encryption, Database Outsourcing, Search Efficiency, and Per-Query Privacy is presented. The comparisons between schemes show that:

#### *a: REGARDING QUERY ENCRYPTION*

*K-anonymity* and *E.C.PSEUDO* do not include query encryption techniques for query privacy preserving, *AMOEB*A and *LPA* adopt hybrid cryptography for query privacy preserving,

TABLE 2. Comparison of privacy-preserving Schemes.

Approach	Comparison Metrics			
	Query Encryption	Database Outsourcing	Complexity of Search Efficiency	Per-Query Privacy
<i>K-anonymity</i>	NO	NO	$O(N^2)$	YES
<i>E.C.PSEUDO</i>	NO	NO	$O(2N^2)$	YES
<i>AMOEB</i> A	YES (Hybrid Encryption)	NO	$O(2N)$	YES
<i>LPA</i>	YES (Hybrid Encryption)	NO	$O(2N)$	YES
<i>POSTER</i>	YES (SWHE)	YES	$O(\log(N+1)^2)$	YES
<i>TK-FHE</i>	YES (FHE)	YES	$O(\log(N+1)^2)$	YES
<i>P<sup>2</sup>FHE-AES</i>	YES (FHE-AES)	YES	$O(\log N)$	YES

*POSTER* adopts somewhat homomorphic encryption for query privacy preserving, *TK-FHE* uses FHE to preserve query privacy, and *P<sup>2</sup>FHE-AES* involves FHE-AES to preserve query privacy.

*b: REGARDING DATABASE OUTSOURCING*

*K-anonymity*, *E.C.PSEUDO*, *AMOEB*A, and *LPA* do not involve database outsourcing techniques to cloud server.

*c: REGARDING COMPLEXITY OF SEARCH EFFICIENCY*

*E.C.PSEUDO* has the highest complexity value of search efficiency because this concept uses temporary pseudonyms to each vehicle which is changed and updated for each request. *K-anonymity* has a very high complexity value of search efficiency  $O(N^2)$  since the query request is published from  $k$  users, therefore the response will reach to the same  $k$  users and it cannot be applied to real-time services. Both *AMOEB*A and *LPA* have  $O(2N)$  complexity values of search efficiency that less than previous schemes because they depend on CGLA. *POSTER* and *TK-FHE* have the same complexity value of search efficiency which is  $O \log(N+1)^2$ . It is less than the previous schemes because they rely mainly on homomorphic encryption which is accompanied with some noise. *P<sup>2</sup>FHE-AES* has the least complexity value of search efficiency  $O \log N$  since it depends on FHE-AES which is noise free.

*d: REGARDING PER-QUERY PRIVACY*

All schemes satisfy this approach with different ways.

2) RESPONSE TIME WITH VARIABLE NUMBER OF VEHICLE USERS

Response time is the time elapsed between the end of an inquiry or demand on a system and the beginning of a

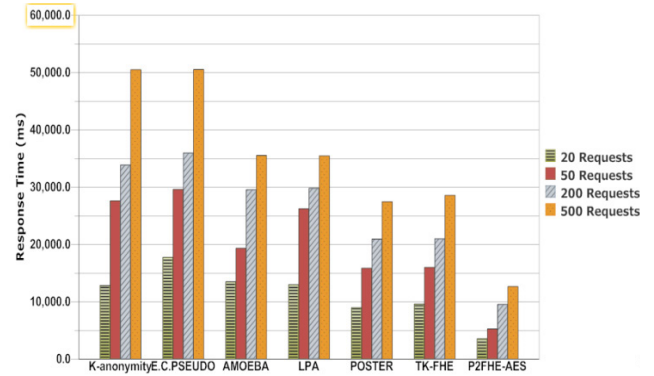


FIGURE 6. Response time.

TABLE 3. Comparison of query response time.

Approach	Number of Query Requests			
	20	50	200	500
<i>K-anonymity</i>	12845.32	27641.52	33875.58	50532.4
<i>E.C.PSEUDO</i>	17781.35	29652.16	35987.35	50547.8
<i>AMOEB</i> A	13520.87	19364.84	29574.94	35536.9
<i>LPA</i>	13014.75	26245.14	29845.17	35499.3
<i>POSTER</i>	9012.63	15890.52	20963.41	27452.58
<i>TK-FHE</i>	9632.42	16026.93	21036.62	28584.97
<i>P<sup>2</sup>FHE-AES</i>	3587.01	5273.53	9563.71	12675.96

response. As shown in Figure 6, the architectures were simulated for varying number of query requests of *VUs* generated (20, 50, 200 and 500) per second. The query request size and query response size are kept fixed. The values of response time of variable schemes are also tabulated in Table 3 to can differentiate obviously between these schemes.

From Table 3, it can be clearly seen that with increasing the number of query requests of *VUs* (i.e., number of request generated /sec) response time is increasing with a rapid rate in all schemes. We notice that *P<sup>2</sup>FHE-AES* scheme has the least time for responding.

3) QUERY ACCURACY

The corresponding accuracy rates of query are very important for identifying the performance of schemes on *VU<sub>i</sub>* and LBSP with variant number of requests. We express *query accuracy* = number of requested query/number of response query. Therefore, the best performance is when accuracy  $\cong 1$ . It is assumed that the worst case happens in the VANET simulation which is formed of 500 vehicles, when all these vehicles send query requests in the same time which leads to bottleneck formation. The results are shown in Figure 7 and Table 4.

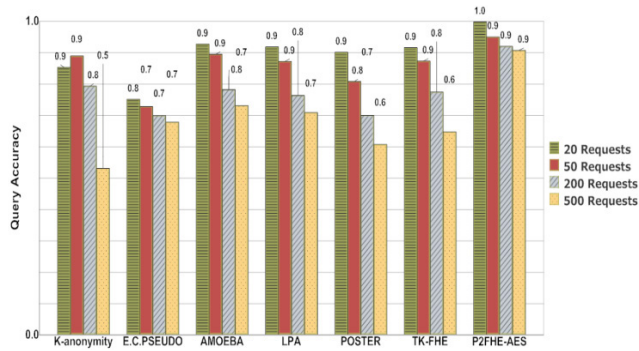


FIGURE 7. Query accuracy.

TABLE 4. Comparison of query accuracy.

Approach	Number of Query Requests			
	20	50	200	500
<i>K-anonymity</i>	0.853	0.889	0.793	0.582
<i>E.C.PSEUDO</i>	0.751	0.728	0.699	0.678
<i>AMOEBa</i>	0.901	0.808	0.739	0.607
<i>LPA</i>	0.916	0.873	0.774	0.647
<i>POSTER</i>	0.927	0.895	0.782	0.731
<i>TK-FHE</i>	0.918	0.872	0.763	0.709
<i>P<sup>2</sup>FHE-AES</i>	0.998	0.931	0.926	0.907

As shown in Table 4, although the performance accuracy of the proposed approach has a little variation when the bottleneck happens, this performance drop is approximately less than 10% and those variations are acceptable. On the other hand, using the proposed approach, accuracy rate is approximately higher than 91% can always be reached with variant number of requests. It is seen also that in the best case (20 query requests), the accuracy reaches about 100%.

4) THROUGHPUT

Throughput of VANET is a measure of the amount of transmitted data from the source vehicle to the destination LBSP and vice versa in the VANET in a unit period of time (second) given by (18):

$$Thr = \sum_{i=1}^n \frac{Nb_i}{T_i} \quad (18)$$

where *Thr* is the throughput of the vehicle, *Nb* is the number of bits transmitted from source to destination, *T* is the time taken for transmission, and *n* is a number of queries.

For each scheme, the throughput is analyzed for 20, 50, 200, and 500 vehicles varying only in the maximum speed of

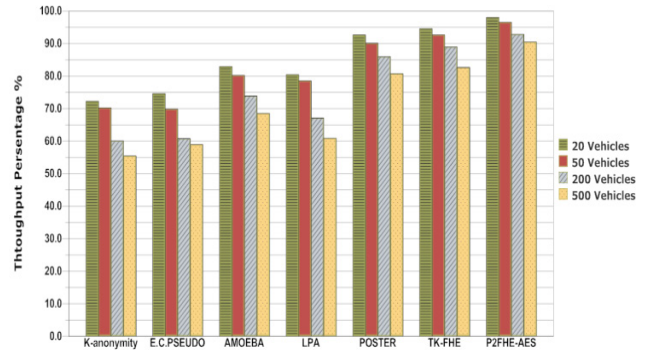


FIGURE 8. Throughput percentage.

TABLE 5. Throughput percentage with different vehicles numbers.

Approach	Number of Vehicles			
	20	50	200	500
<i>K-anonymity</i>	72.24%	70.25%	60.07%	55.54%
<i>E.C.PSEUDO</i>	74.63%	69.84%	60.77%	58.97%
<i>AMOEBa</i>	82.94%	80.22%	73.87%	68.54%
<i>LPA</i>	80.41%	78.54%	67.11%	60.87%
<i>POSTER</i>	92.63%	90.07%	85.95%	80.71%
<i>TK-FHE</i>	94.56%	92.63%	88.97%	82.68%
<i>P<sup>2</sup>FHE-AES</i>	98.05%	96.54%	92.83%	90.47%

vehicles within simulation time 180s. Figure 8 and Table 5 show the throughput percentage with the variant of vehicles number.

As shown in Table. 5, the proposed P<sup>2</sup>FHE-AES scheme is generally expected to give better percentage of throughput followed by *TK-FHE* scheme then *POSTER* scheme because each of *P<sup>2</sup>FHE-AES*, *TK-FHE* and *POSTER* are based on homomorphic approach so that the data delivery rate is higher than the other schemes. The proposed *P<sup>2</sup>FHE-AES* gives the best performance because it sends encrypted query without any noise so that it saves the packet size from increasing and this leads to decreased probability of dropping packets.

5) TIME COST COMPARISON

The comparison of the total time cost results are for the aforementioned four operations Key Generation, Encryption, Evaluation, and Decryption are shown in Table 6. This test has not been performed on *K-anonymity* scheme and *E.C.PSEUDO* scheme because they don't support cryptosystem.

From Table 6, it can be seen that *P<sup>2</sup>FHE-AES* scheme is much more efficient than the others because the time cost

TABLE 6. Comparison of time cost.

Approach	Operation Type			
	KeyGen.	Enc.	Eval.	Dec.
AMOEB A	8563.84	10258.93	Null	9651.2
LPA	8009.71	9632.15	Null	9321.6
POSTER	5285.63	7361.26	5904.51	4852.6
TK-FHE	4521.94	6441.08	4286.01	3879.7
P <sup>2</sup> FHE-AES	1563.22	1003.54	2138.82	732.1

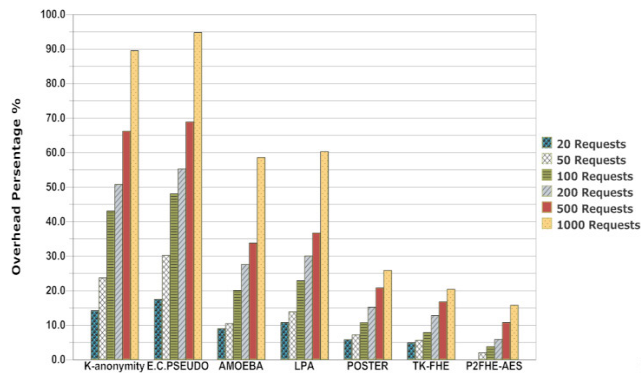


FIGURE 9. Overhead percentage.

in Key generation, Encryption, and Decryption operations is less than in others schemes; although verifying operation takes more time in P<sup>2</sup>FHE-AES scheme.

As expressed in Table 6, there is no evaluation time consumed in AMOEB A and LPA because they are based on hybrid cryptography (which means symmetric and asymmetric cryptography), so that they don't include evaluation function. They just include key generation, encryption and decryption functions. They need much more time to perform this type of cryptography.

6) SYSTEM OVERHEAD COMPARISON

The overhead of location-based services is studied. The overhead is measured as the number of packets transmitted and sent during the location updates, queries and replies. As shown in Figure9, all compared schemes except P<sup>2</sup>FHE-AES, TK-FHE, and POSTER schemes have a large update mechanism because the updates in them are continuous to identify new vehicles entering to communication zone. P<sup>2</sup>FHE-AES, TK-FHE, and POSTER schemes are using a real-life dataset Open-StreetMap. So, LBSP imports directly updated data from dataset. As a result of the overhead comparison as shown in Figure 9, P<sup>2</sup>FHE-AES scheme has less

TABLE 7. Tracing success ratio.

Approach	Number of Query Requests			
	20	50	200	500
K-anonymity	0.421	0.584	0.695	0.804
E.C.PSEUDO	0.786	0.894	0.952	0.985
AMOEB A	0.521	0.638	0.724	0.851
LPA	0.598	0.675	0.775	0.896
POSTER	0.	0	0.324	0.428
TK-FHE	0	0	0.284	0.351
P <sup>2</sup> FHE-AES	0	0	0	0.072

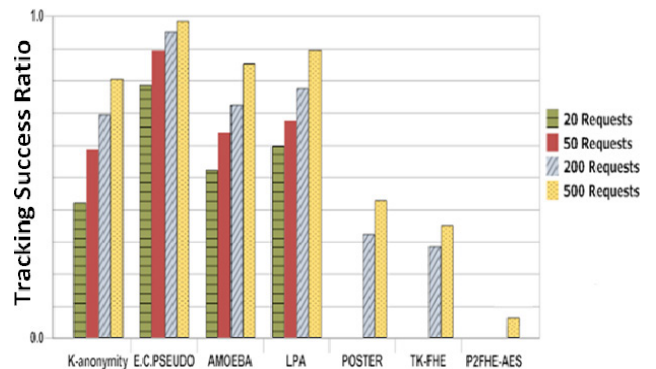


FIGURE 10. Tracing success ratio.

computation time than TK-FHE and POSTER. So that it has the lowest location overhead in general.

7) LOCATION PRIVACY PRESERVING METRICS

Location privacy preserving metrics mean how to measure the level of privacy preservation. In the proposed P<sup>2</sup>FHE-AES scheme, tracking success ratio is used as a metric. Tracking success ratio indicates the possibility that the attacker can track the vehicle query information with variant number of vehicles' query requests. We will refer to tracking success ratio as P, and it can be formed as follows.

$$P = \frac{N_q}{T_q} \tag{19}$$

where N<sub>q</sub> is the number of query requests correctly guessed, and T<sub>q</sub> is the total number of query requests. P can be intuitive to indicate the threaten degree from the network attackers. From (19) we can conclude that, the value of tracking success ratio is a real number between 0 and 1.

P gets higher when it gets close to 1; this means that the attacker have high chance for successful tracking (the worst case).

Figure 10 and Table 7 illustrate the comparison of tracking success ratio of the proposed  $P^2FHE-AES$  scheme with the existing schemes. The proposed  $P^2FHE-AES$  has tiny value of  $P$  at high number of query requests (500 requests), as shown in Figure 10. It means that, this scheme has the highest defense against tracking attack. So that, the attacker is not able to track the query request; because  $P^2FHE-AES$  scheme encrypts the query before being uploaded to LBSP, this prevents query from being tracked. Figure 10 illustrates that, the proposed  $P^2FHE-AES$  has the superiority of preventing location tracking followed by  $TK-FHE$  then  $POSTER$ . The scheme that has the highest  $P$  for location tracking is  $E.C.PSEUDO$  followed by  $LPA$  then  $AMOEBa$  and finally  $K-anonymity$  scheme. Table 7 clarifies the results in more details.

### VIII. CONCLUSION AND FUTURE WORK

In this paper, we addressed the location privacy threats that emerge in VANET system due to unauthorized tracking of vehicles based on their broadcasts, as well as potential user privacy threats due to identification of LBS applications accessed from vehicle. We proposed a scheme, called  $P^2FHE-AES$  solution based on FHE technique over AES symmetric cryptography to prevent noise associated with data, then outsourcing LBS data to the cloud in a privacy-preserving fashion.  $P^2FHE-AES$  scheme allows the LBSP to perform the query request while protecting the privacy of  $VU_s$ ' queries and identity.  $P^2FHE-AES$  scheme also allows the CSP to perform computations over encrypted data to detect the shortest way to the desired destination. So, we keep the service data confidential from RSUs, LBSP, and CSP.

A simple model was designed to study the LBS usage in VANET system and we subsequently created a set up with real traffic scenario of Ismailia city of various node densities, which will help us to analyze the performance metrics of the LBS usage in VANET (response time, query accuracy, throughput percentage, time cost, and overhead percentage). This scenario is implemented and evaluated using NS-2 network simulator and SUMO traffic simulator. A realistic vehicular movement is implemented. Analysis results show that  $P^2FHE-AES$  scheme is performing better in real time and dynamic environment. Query accuracy and throughput reached about 100% and 98% respectively in some cases.

Ongoing work is focusing on applying this security scheme at V2V communication such as cooperative driving to reduce traffic congestion with increasing vehicular safety.

### REFERENCES

- [1] M. Braasch and A. Dempster, "Tutorial: GPS receiver architectures, front-end and baseband signal processing," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 34, no. 2, pp. 20–37, Feb. 2019.
- [2] M. Shengdong, X. Zhengxian, and T. Yixiang, "Intelligent traffic control system based on cloud computing and big data mining," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6583–6592, Dec. 2019.
- [3] R. Attia, R. Rizk, and H. A. Ali, "Efficient Internet access framework for mobile ad hoc networks," *Wireless Pers. Commun.*, vol. 84, no. 3, pp. 1689–1722, Oct. 2015.
- [4] S. Zhankaziev, M. Gavrilyuk, D. Morozov, and A. Zabudsky, "Scientific and methodological approaches to the development of a feasibility study for intelligent transportation systems," *Transp. Res. Procedia*, vol. 36, pp. 841–847, 2018.
- [5] G. Naik, J. Liu, and J.-M.-J. Park, "Coexistence of dedicated short range communications (DSRC) and Wi-Fi: Implications to Wi-Fi performance," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, USA, May 2017, pp. 1–9.
- [6] J. Wang, K. Liu, K. Xiao, X. Wang, Q. Han, and V. C. S. Lee, "Delay-constrained routing via heterogeneous vehicular communications in software defined BusNet," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5957–5970, Jun. 2019.
- [7] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.
- [8] J. Pan, J. Cui, L. Wei, Y. Xu, and H. Zhong, "Secure data sharing scheme for VANETs based on edge computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, Dec. 2019.
- [9] R. Rizk and H. Nashaat, "Smart prediction for seamless mobility in F-HMIPv6 based on location based services," *China Commun.*, vol. 15, no. 4, pp. 192–209, Apr. 2018.
- [10] R. Shokriy, C. Troncoso, C. Diaz, J. Freudigery, and J. P. Hubaux, "Unraveling an Old Cloak: K-anonymity for Location Privacy," in *Proc. 9th Annu. ACM Workshop Privacy Electron. Soc. (WPES)*, New York, NY, USA, Oct. 2010, pp. 115–118.
- [11] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. Eur. Workshop Secur. Adhoc Sensor Netw. (ESAS)*, in Lecture Notes in Computer Science, vol. 4572. Berlin, Germany: Springer, 2007, pp. 129–141.
- [12] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBa: Robust location privacy scheme for VANET," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
- [13] X. Xue and J. Ding, "LPA: A new location-based privacy-preserving authentication protocol in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 69–78, Jan. 2012.
- [14] P. Hu and S. Zhu, "POSTER: Location privacy using homomorphic encryption," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 198. Cham, Switzerland: Springer, 2017, pp. 758–761.
- [15] M. Hur and Y. Lee, "Privacy preserving Top-k location-based service with fully homomorphic encryption," *J. Korea Soc. Simul.*, vol. 24, no. 4, pp. 153–161, Dec. 2015.
- [16] A. Choudhury and A. Patra, "An efficient framework for unconditionally secure multiparty computation," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 428–468, Jan. 2017.
- [17] P. Ah-Fat and M. Huth, "Optimal accuracy-privacy trade-off for secure computations," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 3165–3182, May 2019.
- [18] S. Sahnoud, W. Elmasry, and S. Abudalfa, "Enhancement the Security of AES Against modern attacks by using variable key block cipher," *Int. Arab J. e-Technol.*, vol. 3, pp. 17–26, Jan. 2013.
- [19] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," *J. Electr. Syst. Inf. Technol.*, vol. 2, no. 3, pp. 296–313, Dec. 2015.
- [20] Y. Alkady, F. Farouk, and R. Rizk, "Fully homomorphic encryption with AES in cloud computing security," in *Proc. Int. Conf. Adv. Intell. Syst. Inform. (AISI)*, vol. 845. Cham, Switzerland: Springer, 2018, pp. 270–283.
- [21] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic evaluation of the AES circuit," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 7417. Berlin, Germany: Springer, Aug. 2012, pp. 850–867.
- [22] B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams, "Secure two-party computation is practical," in *Proc. ASIACRYPT*, in Lecture Notes in Computer Science, vol. 5912. Berlin, Germany: Springer, 2009, pp. 250–267.
- [23] Y. Alkady, M. I. Habib, and R. Rizk, "A new security protocol using hybrid cryptography algorithms," in *Proc. 9th Int. Comput. Eng. Conf. (ICENCO)*, Cairo, Egypt, Dec. 2013, pp. 109–115.
- [24] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in *Proc. CRYPTO*, in Lecture Notes in Computer Science, vol. 6841. New York, NY, USA: Springer-Verlag, 2011, pp. 505–524.

- [25] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *Proc. 13th Int. Conf. Pract. Theory Public Key Cryptogr. (PKC)*, in Lecture Notes in Computer Science, vol. 6056. New York, NY, USA: Springer-Verlag, 2010, pp. 420–443.
- [26] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proc. 3rd Conf. Innov. Theor. Comput. Sci. (ITCS)*, vol. 6477, 2012, pp. 309–325.
- [27] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.
- [28] D. McKenney and T. White, "Distributed and adaptive traffic signal control within a realistic traffic simulation," *Eng. Appl. Artif. Intell.*, vol. 26, no. 1, pp. 574–583, Jan. 2013.
- [29] Z. Yong-Xia and Z. Ge, "MD5 research," in *Proc. 2nd Int. Conf. Multimedia Inf. Technol.*, Kaifeng, China, 2010, pp. 271–273.
- [30] S. Chatterjee, A. Menezes, and F. Rodriguez-Henriquez, "On instantiating pairing-based protocols with elliptic curves of embedding degree one," *IEEE Trans. Comput.*, vol. 66, no. 6, pp. 1061–1070, Jun. 2017.
- [31] R. Nitin Chopde and K. Mangesh Nichat, "Landmark based shortest path detection by using A\* and haversine formula," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 1, no. 2, pp. 298–302, Apr. 2013.
- [32] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, Jun. 2013.
- [33] B. Lynn. (2015). *The Pairing-Based Cryptographic Library*. Accessed: Jan. 1, 2020. [Online]. Available: <http://crypto.Stanford.edu/pbc/>
- [34] W. Hart, F. Johansson, and S. Pancratz. (2013). *FLINT: Fast Library for Number Theory, Version 2.4.0*. [Online]. Available: <http://flintlib.org>
- [35] M. Varia, S. Yakubov, and Y. Yang, "HEtest: A homomorphic encryption testing framework," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence Bioinformatics), vol. 8976. Berlin, Germany: Springer, 2015, pp. 213–230.
- [36] OpenStreetMap Contributors. (2017). *Planet Dump*. [Online]. Available: <https://planet.osm.org>
- [37] (2008). *NS-2 2008 The Network Simulator—NS 2*. Accessed: Jan. 1, 2020. [Online]. Available: <https://www.isi.edu/nsnam/ns/>
- [38] *SUMO-Simulation of Urban Mobility*. Accessed: Jan. 1, 2020. [Online]. Available: <http://sumo.sourceforge.net/>
- [39] *CloudSim*. [Online]. Available: <http://www.cloudbus.org/cloudsim/>



**FIFI FAROUK** received the B.Sc. and M.Sc. degrees in computer and control engineering from Suez Canal University, in 2001 and 2008, respectively, and the Ph.D. degree in computer and control engineering from Port Said University, in 2014. She is currently a Lecturer with the Technology and Information Systems Department, Port Said University, Egypt.



**YASMIN ALKADY** received the B.Sc. degree in computer and control engineering from Suez Canal University, in 2007, and the M.Sc. degree in computer and control engineering from Port Said University, in 2014, where she is currently pursuing the Ph.D. degree. She has been an IT Engineer with Medical Union Pharmaceuticals (MUP) factories, since 2014.



**RAWYA RIZK** received the B.Sc., M.Sc., and Ph.D. degrees in computers and control engineering from Suez Canal University, in 1991, 1996, and 2001, respectively. She was the Executive Director of the PSU Network Infrastructure, Port Said University, Egypt, from 2010 to 2014. She was the Manager of the CISCO Academy, Faculty of Engineering, Suez Canal University, from 2008 to 2010. She has been the Manager of the CISCO Academy, Faculty of Engineering, Port Said University, since 2010, the Chief Information Officer (CIO) of Port Said University (PSU), since 2014, and the Head of the Electrical Engineering Department, Port Said University, since 2017. She is currently a Professor of computers and control with the Electrical Engineering Department, Port Said University. Her research interest is in computer networking, including mobile networking, wireless, ATM, sensor networks, ad hoc networks, QoS, traffic and congestion control, handoffs, and cloud computing. She is a Reviewer in many of international communication and computer journals, such as the *IEEE Access*, *IET Communications*, *IET Sensors*, *IET Networks*, *Journal of Supercomputing*, *Journal of Network and Computer Applications*, *Computers and Electrical Engineering*, *Mathematical Problems in Engineering*, and *IJACSA*.

• • •