Framework of Geofence Service using Dummy Location Privacy Preservation in Vehicular Cloud Network

Hani Al-Balasmeh
Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, India
hbalasmeh_phd17@thapar.edu

Maninder Singh
Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, India
Msingh@thapar.edu

Raman Singh
School of Computing, Engineering, and Physical Sciences, University of the West of Scotland, United Kingdom
Raman.Singh@uws.ac.uk

Abstract: *With the increasing prevalence of different mobile apps, many applications require users to enable the location service on their devices. For example, the geofence service can be defined as establishing virtual geographical boundaries. Enabling this service triggers entering and exiting the boundary area and notifies the users and trusted third parties. The foremost concern of using geofence is the privacy of location coordinates shared among different applications. In this paper, a framework called 'TIET-GEO' is proposed that allows users to define the geofence boundary; in addition, it monitors Global Positioning System (GPS) devices in real-time when they enter/exit a specific area. The proposed framework also proposes a dummy privacy preservation algorithm to generate K-dummy locations around the real trajectories when the user requests the Point Of Interest (POI) from the Location-Based Services (LBS). This article aims to enhance the location privacy preservation in geofence service, by generating a k-dummy location around the user location based on the radius size of the geofence area. The proposed framework uses token keys authentication to authorize the users in the Vehicular Cloud Network (VCN) service by generating secret token keys authentication between the client and services. The results obtained show the effectiveness of the proposed framework was on parameters like flexibility and reliability of responses from different sources, such as smart IoT devices and datasets.*

Keywords: *Location privacy preservation, geofence service, vehicular cloud, user-authentication.*

Received February 10, 2022; accepted April 13, 2022
https://doi.org/10.34028/iajit/20/1/8

1. Introduction

Location-based services are supported by the Global Positioning System (GPS) and benefit users by providing the current location or Point Of Interest (POI) and the destination route. In geofence, a virtual boundary is created around a specific physical location or point on a map. Geo-fencing uses GPS coordinates to define an area; it captures the device's latitude and longitude to determine the coordinates and trigger specific actions depending on whether the device is inside or outside that virtual boundary area. A predefined action is triggered by sending specific messages. A geofence is defined as the user entering or exiting at a particular time, as shown in Figure 1.

Figure 1. Geofence triggering events.

Geo-fencing services have several applications, such as marketing, security, smart roads, and smart cities. In marketing, indoor mobile positioning applications are popular and provide significant value, especially for department stores, shopping malls, and airports. In smart roads, geo-fencing reduces traffic congestion by providing alternative routes to vehicles and by displaying probable accident zones. In vehicular network services, the GPS and Location-Based Services (LBS) systems are used in most services provided to vehicles on the road, such as destination, location, navigation systems, and vehicle tracking. In this paper, we propose a real-time geofence services framework called TIET-GEO in vehicular networks. The framework can define geofence boundaries in a specific area and monitor the GPS devices when they enter or exit the geofence area in real-time. The framework provides email notifications to the users or trusted third parties in case of any triggers. The proposed framework enhances location privacy preservation by using the dummy location generation technique. Generates the 'k' number of dummy locations around the real location and sends them to LBS to request the location coordinates.

The rest of this paper is organized as follows. In section 2, related and recent research from various researchers is discussed. The proposed framework and the different methodologies used are explained in section 3. Security mechanisms such as dummy location generation and authentication communication used in the proposed framework are described in section 4 and the results are discussed in section 5. Finally, the conclusions are presented in section 6.

2. Related Works

Agarwal *et al*. [1] proposed a novel localization application to prevent collisions on the roads, detect accidents, and estimate the time of arrival. The application was an intelligent traffic monitoring system based on cloud mobile applications; it introduced algorithms to implement real-time safety applications in vehicular networks. Proposed a novel quorum-based location service scheme in vehicular sensor networks comprised of vehicles and sensor nodes on the roads [32]. The scheme provides information about the vehicles and nodes by using a combined quorum of location queries and location updates to define a quadrangular path on the route and at crossing points. Proposed a novel cooperative localization technique for vehicles equipped with high-position accuracy GPS, and the technique utilizes the Round Trip Time (RTT) for inter-vehicle distance calculation [8]. However, the problem of the accuracy of space-time information in positioning vehicles in-vehicle networks remains unsolved [11] resolved this by proposing a high precision-based vehicle network location service; this service uses the wide-area precise positioning technology. A concurrence service system is developed to ensure the reliability of data exchanged between the vehicles; in addition, background verification of the positioning precision quality in an urban environment is performed. Proposed a logistics management model called 'SafeTrack' to manage vehicles by monitoring them in real-time by using the geofence algorithm and radiofrequency technology [20]. In this approach, the researchers focused on ensuring delivery management by monitoring detours on planned routes and addressing notifications. Introduced a novel method to formalize sophisticated geofencing scenarios as a state; it considers temporal relations between geofence areas when a user moves between geofence areas by providing smart notifications of a user accessing multiple geofence areas [21]. Introduced a prototype of a service-oriented platform to track mobile devices in real-time and integrate geofencing techniques. The prototype can define adequate and safe itineraries for any vehicle [16]. Cheng *et al*. [5] proposed a novel collaborative geofence site selection technique that provides an optimal method for city management. The novel manages dockless shared bikes in the city and optimizes the distribution locations and the occupied area for each geofence. Proposed a fine-grained indoor geo-notification system called "iGeoNoti" that uses the pedestrian reachable distance. Using this method, the geo-notifications are not limited, and the indoor geofence can be implemented across multiple floors [34]. However, location-dependent actions are not triggered when users enter or exit a geofence area [9] proposed a method to increase the reliability of a proactive LBS and to provide valuable estimations by ensuring quantifiable and predictable reliability for people unfamiliar with technology. In addition, they determined the process used by a proactive LBS to execute a location-dependent action when a user crosses a geofence area. By using point-to-multipoint device-to-device communications to provide rapid and reliable geofence broadcasts in LTE-advanced networks and to support critical services of vehicular collision alerts, Nardini *et al*. [17] proposed a novel approach to broadcast device-to-device messages over multiple cells; and the approach relies on centralized decisions and uses the eNodeBs infrastructure to schedule unsolicited device-to-device communication and to ensure optimal implementation of user equipment by forwarding messages at any time. To enhance the online shopping experience of customers based on geographical location, Durst *et al*. [7] presented an innovative concept that combines location-based crowdsourcing; it uses geofencing technology to evaluate customers' online shopping experience using cell phones in specific areas. Many phone services facilitate various mass-market GPS-based applications. Greenwald *et al*. [10] presented an economically viable geofencing solution that supports multiple geofence areas that serve large populations. The technical viability is based on actual traffic data obtained from mobile proximity marketing and social network services. Dummy privacy preservation aims to secure the user's real location by sending dummy locations to a service provider along with the real location. Several dummy techniques have been applied by different researchers to enhance the location privacy of users. Some of these techniques can secure the movement trajectories and blur the users' locations to ensure privacy and safety. Liu and Wang [14] proposed a dummy k-anonymous method for the anonymous region area by selecting the k-1 anonymous dummy location based on the location of the user. Requesting dummy query sequences, Wu *et al*. [30] proposed a scheme for user privacy protection in LBS to hide their true location when they are requesting POI from the LBS services. The Hara *et al*. [12] proposed a location privacy preservation method to anonymize the location of a user with an LBS-based mobile device by generating dummy locations in real-time. By ensuring privacy and anonymity of the location, Niu *et al*. [19] Proposed two clocked dummy-based methods to achieve k-anonymity for users with LBS-based devices. The method blurred user coordinates based on a virtual circle or grid into dummy positions based on the entropy-based privacy metric. To ensure the privacy of user trajectories, Wu *et al*. [29] proposed a privacy model called 'adaptive uniformly distributed dummy trajectories' to derive uniformly distributed dummy trajectories. Dummy trajectories are generated by ensuring robust privacy preservation. Wu *et al*. [28] suggested a method to reduce the complexity of dummy location selection and to enhance the privacy of the similar query probability of dummy locations. In this method, the clocking area is selected by enlarging the dummy locations. Considering the problem of privacy preservation mobile trajectories on social networks, Ni *et al*. [18] proposed a privacy preservation R-constraint dummy trajectory. This method ensures that the generated R of the dummy positions is within a specific range and similar to the real location trajectories. By providing trajectory privacy preservation based on fog cloud location services, Wang *et al*. [27] proposed a fog server to store semi-essential data that is physically accessible to the users. In addition, they proposed a dummy rotation anonymity method to enhance the privacy preservation of users' trajectories. In obfuscation of the location trajectories, Al-Balasmeh *et al*. [2] proposed a framework to generate a k-dummy location to obfuscate the user location trajectories in the vehicular cloud network. Proposing a Multilevel Location Privacy Scheme (MLPS) to anonymize the vehicle location when exchanging the location with LBS services [26]. Proposing a scheme of anonymous and unlikable participation of the IoV location trajectories by Concerted Silence-Based Location Privacy Preservation for the internet of vehicles (CSLPPS) in the vehicular networks [4]. Increase leakage of the location data of the vehicle's trajectory's location from the vehicular ad-hoc network, the researcher proposed a Virtual Trajectory Generation algorithm (VTG). The proposed VTG provides privacy production of the users' trajectories by connecting true position with virtual points when requesting from the LBS [3]. Based on using a key agreement protocol to provide privacy preservation for IoT services, Cho and Kim [6] proposed an efficient securing of services based on a symmetric key cryptosystem for IoT services. Table 1 shows the summary of the related works.

Table 1. Summary of the related works.

Auth	Proposed	Method	Description
[1]	novel localization application	NA	To prevent collisions on the roads, detect accidents, and estimate the time of arrival in vehicular networks.
[34]	novel quorum-based location service	NA	The scheme provides information about the vehicles and nodes by using a combined quorum of location queries in vehicular sensor networks.
[8]	novel cooperative localization technique	NA	Equipped with high-position accuracy GPS of the vehicles.
[11]	high precision-based vehicle network location service	NA	Provides the reliability of data exchanged between the vehicles; in addition, background verification of the positioning precision quality in an urban environment.
[20]	SafeTrack	NA	a logistics management model proposed to manage vehicles by monitoring them in real-time by using the geofence service and ensuring delivery notifications.
[21]	a novel method to formalize sophisticated geofencing	NA	Providing smart notifications of a user accessing multiple geofence areas.
[16]	prototype of a platform to track mobile	NA	The prototype can define adequate and safe itineraries by tracking the devices in real-time.
[5]	novel collaborative geofence	NA	The novel manages dockless shared bikes in the city and optimizes the distribution locations and the occupied area for each geofence
[5]	iGeoNoti	NA	Proposed a fine-grained indoor geo-notification system. Using this system, the geo-notifications are not limited, and the indoor geofence can be implemented across multiple floors.
[34]	method to increase the reliability of a proactive LBS	NA	They determined the process used by a proactive LBS to execute a location-dependent action when a user crosses a geofence area.
[9]	a novel approach to broadcast device-to-device messages over multiple cells	NA	Enhance the online shopping experience of customers based on geographical location by forwarding messages at any time to users.
[17]	presented an innovative concept of location-based crowdsourcing	NA	To evaluate customers' online shopping experience using cell phones in specific areas using geofence technology.
[7]	Presented economically viable support for multiple geofences.	NA	Provides a solution that supports multiple geofence areas that serve large populations. The technical viability is based on actual traffic data obtained from mobile proximity marketing and social network services.
[10]	Dummy query sequences scheme	Dummy, K-anonymity	Proposed scheme to provide the location privacy queries when the user requests the location from the LBS service.
[14]	All-dummy k-anonymous scheme	Dummy, k-anonymity	Proposed construct anonymous regions by selecting a k-1 location and real users based on location offset.
[12]	proposed a location privacy preservation method	dummy locations	To anonymize the location of a user with an LBS-based mobile device by generating dummy locations in real-time.
[19]	proposed two clocked dummy-based in LBS	Dummy, K-Anonymity technique	The method blurred user coordinates based on a virtual circle or grid into dummy positions based on the entropy-based privacy metric.

[29]	Adaptive uniformly distributed dummy trajectories model	Dummy	to derive uniformly distributed dummy trajectories of the user movements.
[28]	method to reduce the complexity of dummy location selection	Dummy selection	To enhance the privacy of the similar query probability of dummy locations, by selecting the clocking area in the mobile trajectories on social networks.
[18]	a privacy preservation R-constraint dummy trajectory	Dummy	Generated R of the dummy positions is within a specific range and similar to the real location trajectories based on fog cloud location services.
[27]	a dummy rotation anonymity	Dummy, Anonymity	To enhance the privacy preservation of users' trajectories in fog server and provides access to the semi-essential data in the cloud.
[2]	Data and location privacy (DLP)	obfuscation	A proposed framework to obfuscate the user trajectories in vehicular cloud networks, by obfuscation of the locations.
[26]	MLPS	obfuscation	Proposed MLPS obfuscation scheme to provide location privacy of vehicle location.
[4]	CSLPPS	Anonymity	Proposed CSLPPs to anonymize the user trajectories and unlikable participation of IoV.
[3]	VTG	Anonymity	Proposed VTG to generate virtual points and connected they're with true location when requesting from the LBS.
[6]	NA	Hash, ECC, cryptosystem	proposed an efficiently securing services based on a symmetric key cryptosystem for IoT service

3. The Architecture of the TIET-GEO Framework

This section outlines the architecture of the proposed framework and the main problem of location privacy is addressed in geofence services. There is a requirement to provide the privacy of user location over the vehicular cloud network, when the users enter boundaries, the untrusted services can access the location of the mobile devices which can be a serious security vulnerability. Some of the earlier proposed systems like [31] work only for outdoor GPS, and there is no location privacy of users' trajectories when the user enters or exit the geofence areas. The proposed TIET-GEO is proposed to address this issue. There is a need to propose an approach to provide location privacy of users' trajectories of user movement when requesting a POI from the LBS. The proposed framework can be used to monitor several types of IoT GPS devices in indoor or outer geofence areas. The architecture of the proposed TIET-GEO framework consists of six components. The interaction demon-striation of these components is shown in Figure 2.

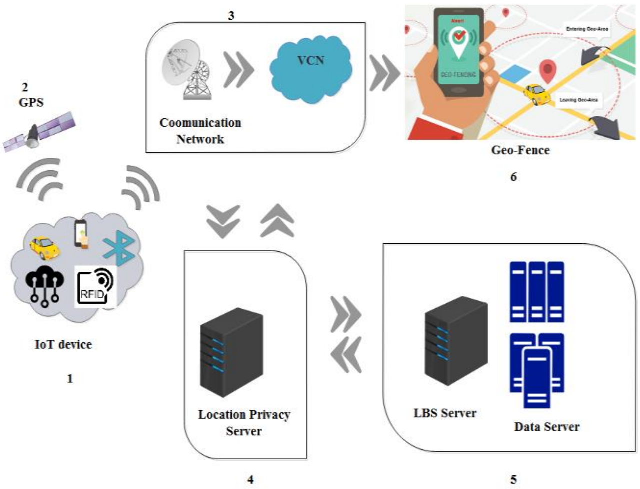

Figure 2. The architecture of the proposed framework.

The various parts of this framework are explained as given below. The first component is the devices (IoT, infrared) used by users. Most smart devices, such as smartphones, smart vehicles, and wearable devices, are equipped with a GPS module to obtain the real-time location or directions from LBS services. The second component is GPS satellites which are widely used to provide the location (Lat, Long), including the date and time, for any GPS-enabled device. The third component is communication networks and vehicular cloud networks. It includes the wireless, global system for mobile and local networks, which are essential for the first hop of transmitting data to the vehicular cloud network over the internet to store the data over the vehicular cloud database. The fourth component is the location privacy server where is provides the location trajectories of the user movement while requesting the POI from LBS services. The fifth component is the LBS server which has the responsibility of providing the location information of the requesting devices and the nearest point of the POI. The last component is the Graphical User Interface (GUI) of the TIET-Geo to provide the geofence services and notifications module. This service displays a user's location on the map and allows the users to monitor their movement in real-time; in addition, it allows the users to define a geofence area on the map and receive email/SMS notifications when a device enters or exits a specific geofence zone. The structure of the framework in Figure 3 shows the stages of accessing TIET-GEO services through vehicular networks.

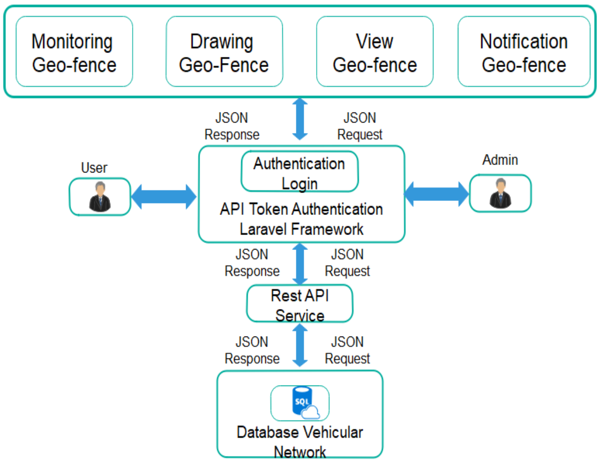

Figure 3. TIET-GEO structure.

The proposed TIET-GEO allows different types of smart IoT devices, such as smart vehicles, smartphones, wearable devices, or any GPS-equipped device, to be identified in the system. The proposed framework is tested using android smartphones, one IoT GPS device, and two different datasets: Manhattan-taxi-trajectories [25], Citi Bike [24] and Geolife GPS trajectories [33]. The proposed framework consists of various functionalities like registration of IoT devices, real-time monitoring, geofence area boundary control, displaying geofence areas, and geo notifications. In the TIET-GEO, used the geofence drawing tools like (marker, circle, polygon, rectangle, and polyline) to define a particular geofence area and monitor it. Let's consider the user defines a circular geofence area with an initial location (lat, long) and expands the circle to obtain the dynamic radius, which is measured in meters. After drawing and defining the geofence area, the circle is stored in the database and is assigned a unique id. The proposed method to display the geofence area on the Maps is based on the haversine formula; in this method, the center of the circle (lat, long) is selected; the radius r of the geofence circle (miles) is obtained from the database. The radius of the earth can be calculated by $r/$ 3956, which can be used to calculate the distance between two points. The latitude and longitude are obtained using the mathematical equations:

$$lat_2 = asin\,(sin(lat_1) \,*\, cos\,(radius) \,+\, cos\,(lat_1) \,*\, sin(radius) \,*\, cos\,(tc))\ and\ lon_2 \,=\, lon_1 \,-\, asin(\,sin\,(tc) \,*\, sin\,(radius)\,/\,((cos\,(lat_1) \,+ Pi)\,\%\,(2 \,*\, Pi) \,-\, Pi)).$$

Finally, a circle is plotted on the map using ploy=vepolyline (989, location, vecolor (33, 255, 0,5), 4) and it is shaded. The procedure is defined in Algorithm (1).

Algorithm 1: Define geofence area.

```
Result: Define geofence area.
Require: latitude, longitude, radius, Pi ← 3.1415926535898
Start:
Select ← IoT device Then:
Function ( lat, long, r)
    Body
  location ← Array [Coordinates]
    $lat_1$ ← lat * Pi / 180
    $long_1$ ← long * Pi / 180
    radius ← r / 3956
    for x ← 0 to x < = 360 do
        tc ← ( x / 90) * Pi
        $lat_2$ ← asin (sin($lat_1$) * cos (radius) + cos ($lat_1$) * sin(radius) * cos (tc))
        $lat_2$ ← 180 * $lat_2$ / Pi
        If ( cos ($lat_1$) == 0) Then
            $lon_2$ ← long
        Else
            $lon_2$ ← $lon_1$ – asin( sin (tc) * sin (radius) / ((cos ($lat_1$) +Pi) % (2 * Pi) – Pi ) )
        End if
            $lon_2$ ← 180 * lon / Pi
            newlocation ← newloc ( $lat_2$ , $lon_2$ )
      End for
                location.push(newlocation)
                ploy ← vepolyline (989 , location, vecolor (33,255,0,5) , 4)
                return poly
    End function
```

3.1. Geo-Targeting Notification

The proposed framework provides smart trigger notification of the IoT devices when the device enters or exits the virtual boundary geofence area. The trigger calculates the difference between two points of the coordinates of the virtual circle forming the geofence and the coordinates of user location to determine whether the device is inside the circle or outside. The flow chart in Figure 4, shows the notifications when the user's location changes which indicates the user or device is entering or exiting a specific geofence area.

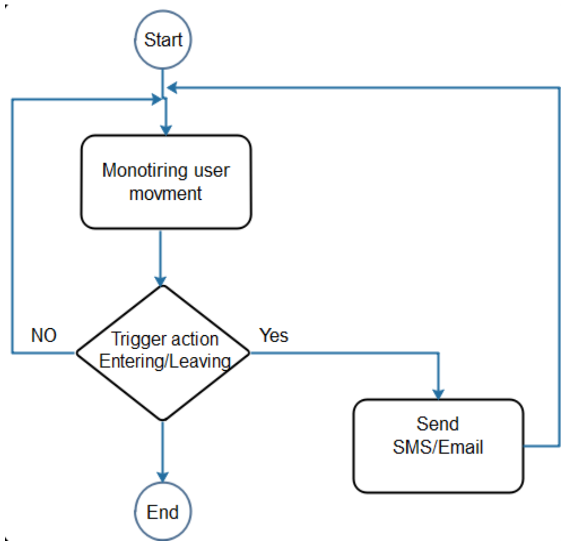

Figure 4. Trigger geofence flow-chart.

On successful implementation, any actions of entering or exiting a particular geofence area are triggered based on the GPS trajectory; notifications are sent to the users or trusted third parties about such actions within the geofence. The user receives the coordinates (latitudes 2, longitudes 2) for every location movement from the LBS. Let's assume the central angle between any two points on the sphere can be defined as

$\Theta\ = d/r$, where “d” is the distance between the two points along with a circle of the sphere, and “r” is the radius of the sphere. By using the haversine formula, $\Theta = haversine(\Delta\Phi) +\ cos(\Phi_1) * cos(\Phi_2) + haversine(\Delta\lambda)$, where the radius of the earth is r=6371 km, and the different distance between the two points of the latitude is $\Delta\Phi\ =\ \Phi_2\ -\ \Phi_1$, and the difference between the two points of longitude is $\Delta\lambda\ = (\ \lambda_{\ 2} - \lambda_1\ )$. As shown in Figure 5, the central angle between the two points P and Q is represented by $\Delta\sigma$, and Φ and λ are the latitudinal and longitudinal angles of P, respectively.

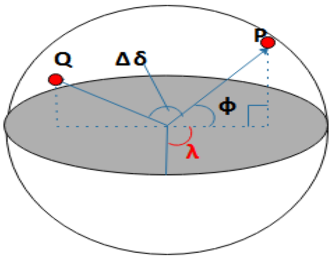

Figure 5. An illustration of the central angle between two points.

If the distance between two points is less, there is a large rounding error when the spherical law of cosines formula is applied. By using the modern 64-bit floating-point number, the rounding errors are insignificant for distances larger than a few meters on the surface of the earth. The have sine formula agrees well for the smallest distances between two points as:

$$\Delta\sigma\ = 2 * arcsin\sqrt{sin^2(\frac{\sqrt{\Delta\Phi}}{2} + cos\Phi_1 * cos\Phi * \sin(\frac{\Delta\lambda}{2})}$$

The step-wise explanation is given as algorithm 2.

Algorithm 2: Geo-Targeting of the geofence area.

```
        Result: Trigger the geofence area
Require:  GPS <$\Phi_2$ ,$\lambda_2$ > ,geofence< $\Phi_1$ ,$\lambda_1$,radius>,
 Pi ← 3.1415926535898
Start:
Function get_dictance  ($\Phi_1$ ,$\lambda_1$, $\Phi_2$ ,$\lambda_2$ )
   Body
   Geo_lat ← $\Phi_1$ * Pi)/180.0
  GPS_lat ← $\Phi_2$ * Pi / 180.0
 diff ← Geo_lat – GPS_lat
di ← ($\lambda_1$ * Pi / 180 ) – ($\lambda_2$ * Pi / 180 )S ← 2 *asin ( sqrt ( pow (sin ( di / 2) , 2 ) + cos ( Geo_lat) * cos ( GPS_lat) * pow ( sin( di / 2),2 )
S ← S * 6378.137
S ← round ( S * 1000 , 3)
Return S
End function
```

3.2. Authentication Service Approach

Security token service based on authentication is popular on web services, where authentication provides a system control to verify the user’s credentials and determine whether access should be authorized by authentication data from the users. Authentication is essential to provide secure access and protect resources when users access the service. Users are usually identified with a user ID/email, and authentication is accomplished when the user provides appropriate credentials, such as provide a password that matches the user ID. For almost every web service that uses an Application Program Interface (API), a token is the best method to manage authentication for multiple users. The proposed secure communication authentication user login framework is based on the open-source ‘laravel’ PHP framework that is used to develop high-end web applications and provide secure authentication of user login. The TIET-GEO framework has been developed using token-based authentication of multiple users logging into a system. The framework secures the communication between the client and the Vehicular Cloud Network (VCN) when the user tries to log in. The login credentials are validated by verifying the user ID and password with the credentials stored in the database on the server-side in an encrypted format. Relevant data are transmitted to the client by using the token key before access is provided to the user. A token authentication is a powerful approach that can ensure a lower load on the server to store multiple session IDs of users on the server by generating tokens for each user after they provide the appropriate credentials. The initial token authentication can be performed using the username and password credentials and the API key or even tokens from another service. As shown in Figure 6, token-based authentication occurs after the user’s credentials are exchanged for a token on the server-side; the client can use the tokens to validate each subsequent request.

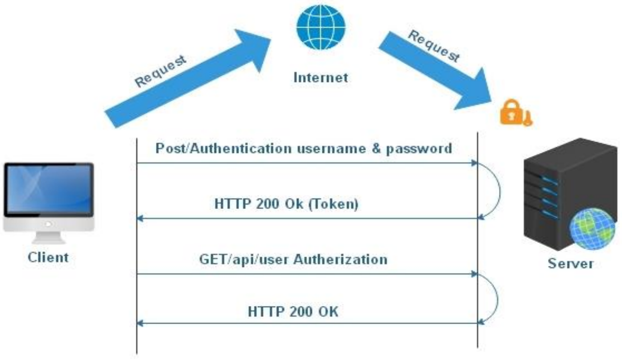
Request
Internet
Request
Post/Authentication username & password
HTTP 200 Ok (Token)
GET/api/user Autherization
HTTP 200 OK
Client
Server

Figure 6. Token-based authentications.

Token-based authentication is stateless and does not store any information about the users on the server-side or during the session. This method is implemented in five steps: User requests access using user ID and password, Service validates credentials, Service provides a token to the user, User stores that token and sends it to the server with every request, and the server verifies the token and provided data in response. Figure 7 shows the workflow of token-based authentication communications between the client and the server.

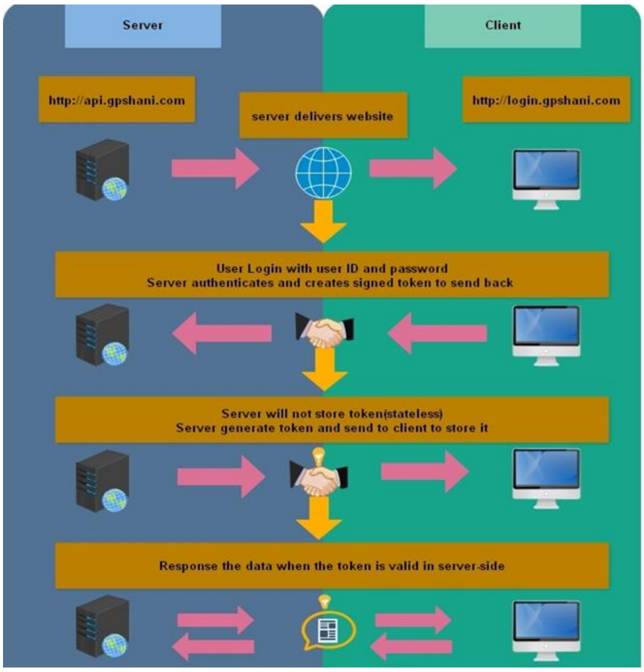
Server
Client
http://api.gpshani.com
server delivers website
http://login.gpshani.com
User Login with user ID and password
Server authenticates and creates signed token to send back
Server will not store token(stateless)
Server generate token and send to client to store it
Response the data when the token is valid in server-side

Figure 7. Workflow of token-based authentication.

The Laravel framework [23] offers a rich functionality method to provide token authentication and encrypts plain text in messages and secures the information during the exchange between the client and the server. The proposed method is based on token authentication user login into the system and encrypting the process information using 'cryptography plain text'; the Laravel framework is developed to use AES-256 and AES-128 encryption, which uses open SSL encryption to ensure secure communication between the client and the server-side.

4. The Dummy Location Generation Approach

Security threats based on location privacy have increased in our daily life with an increased prevalence of LBS and location providers. Dummy techniques are used to provide fake locations and hide the real location of the users. Different dummy techniques are used to ensure location privacy, such as generating dummy locations, dummy trajectories, and dummy locations in a neighborhood. In this paper, we focused on dummy-based approaches to anonymize the actual user locations to generate dummy locations in addition to the actual location of the user in a virtual circle, which are then transmitted to the LBS provider. The proposed method is a circle-based dummy generation method (nearby location). Hayashida *et al*. [13] proposed an algorithm that can ensure the anonymity of the user-defined area and remove the unrealistic assumptions about the user's movements; the user is only required to enter a set of visiting points of their trajectory. Skala and Majdisova [22] proposed dummy selection based on the maximum and minimum distance, and simplified the maximum and minimum distance in both semantic diversity and physical dispersion of locations. Lu *et al*. [15] proposed generating privacy awarded dummy based on either a virtual grid or a circle to protect the location privacy of the mobile user in a mobile system. This approach requires a lightweight server-side front-end to integrate with the existing mobile service systems on the client and server sides. In our method, the dummy locations are based on virtual circular dummy generation; N dummy locations are generated around the user location based on the radius of the geofence in Algorithm (1). The user location and dummy locations are constrained by a virtual circle with radius r and are centered at the position of the user location (loc). The center loc is determined based on the user location in the database. User locations can be used to generate N dummy locations around the Pos based on the value of r. Our method was tested to generate a k number of dummy locations automatically around the user's location to hide the real location. Random points were generated uniformly and independently within a virtual circle of radius r around the location (x_0, y_0); two independent uniform random values u and v were generated in the interval [0,1]. The degree of the geographic coordinates of the location (lat, long), where Φ is the longitude, and is the latitude, with radius r can be measured in meters or feet or another linear measurement unit. The r is converted into a degree if it is located near the equator, that is, approximately 111, 300 meters in degree. The uniform distribution of the dummy random points is obtained to compensate for the distance, $= r\sqrt{u}$, to decrease the statistical bias in the number of points near the center Pos. The angles between the points Pos' can provide radians in a full circle by using $t = 2 * Pi * v$, which can provide angles between 0° and 360°. The trigonometry of dummy location points can be calculated using the random distance and angle obtained using $\Phi_1 = w * cos(t)$ and $\lambda_1 = w * sin(t)$, where the dummy points $P\,os'$ (Φ_1, λ_1) indicate the random distance between the original coordinates and the direction of t. The variation of the distance between the longitude line in $\sigma = \Phi_1 / cos\,(\lambda_0)$ is compensated using the trigonometry of Φ_0 by converting it to radians cos (). During the generation of dummy location points, Pos' $(\Phi_{new,}\, \lambda_{new})$ becomes $\Phi_{new} = \Phi_0 + \sigma$ for the latitude and $\lambda_{new} = \lambda_0 + \lambda_0$ for the longitude. As shown in Figure 8, for k=8 dummy locations and Pos user location all locations, all the locations are constrained by a circle centered at $(Pos, Pos') \leq r$. The positions are distributed to ensure that all θs are equivalent, and every pair of clockwise consecutive and Pos'.

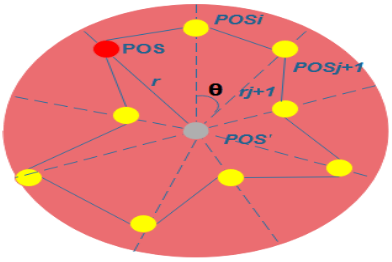

Figure 8. Dummy circle-based.

Figure 9 shows the trajectories of user movement by generating nearby dummies.

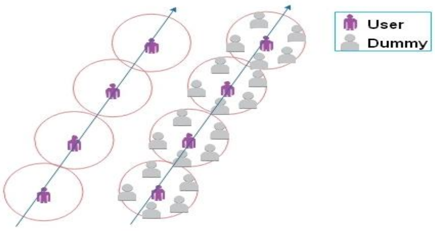

Figure 9. Dummy trajectory of user location.

The proposed method (as given in Algorithm (3)) can secure the real user location in every next movement of the trajectory by providing a k dummy of locations around the user location within a specific radius of the geofence.

Algorithm 3: Dummy Generation locations Privacy.

```
Result: Generates K number of dummy locations around the user location
Require: Pos ( $\Phi$ , $\lambda$ ) , r , Pi $\leftarrow$ 3.1415926535898,
Start:
for N $\leftarrow$ 0, in Pos do
Select $\Phi$ , $\lambda$ , r
K= r / 2
Dummy ( $\Phi$ , $\lambda$ , r , k)
Function Dummy ($\Phi$ , $\lambda$ , r , k) Then
  D $\leftarrow$ r / 111300.0
      for j $\leftarrow$ 0 in k  do
        $\lambda_0 \leftarrow \lambda$
        $\Phi_0 \leftarrow \Phi$
        u $\leftarrow$ random ()
        v $\leftarrow$ random ()
        w $\leftarrow$ r * sqrt( u )
        t $\leftarrow$ 2 * Pi * v
        $\Phi_1 \leftarrow$ w * cos(t)
        $\lambda_1 \leftarrow$ w * sin(t)
        $\sigma \leftarrow \Phi_1$ / cos ($\lambda_0$)
        $\lambda_{new} \leftarrow \lambda_0 + \lambda_1$
        $\Phi_{new} \leftarrow \Phi_0 + \sigma$
        for i $\leftarrow$ 0 in k do
             Plot ($\Phi_{new}$, $\lambda_{new}$)
End for
    End for
   End for
  End function
```

5. Results and Discussion

The proposed framework is tested in the vehicular cloud network environment and imports database servers from servers in real-time. The results show the efficient and flexible response to the location requests from smart IoT devices or smartphones. This section discusses the results obtained by testing different scenarios using the proposed framework. Scenario 1: In this scenario, different smart IoT and infrared devices are considered for monitoring and triggering the action indoors and outer of the particular geofence area. The proposed framework allows the user ability to define and monitor multiple geographical distant geofence areas, accessing the dataset. The users can trigger any action of entering or exit of a particular area and notifying the users over email. Figure 10 shows the number of devices that have been defined in the geofence area and the number of trigger actions in the particular area. Figure 11 show the trigger action of devices in different geofence area.

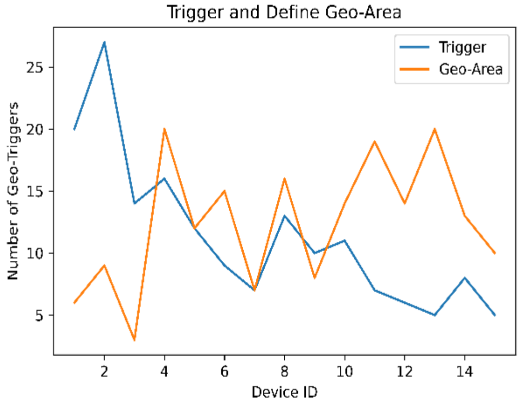

Figure 10. Number of the trigger in the geofence area.

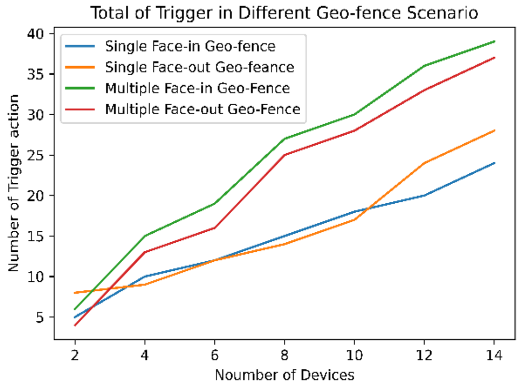

Figure 11. Total of trigger in different geofence scenarios.

Scenario 2: A scenario of triggering the action of entering or exiting the geofence area of Overlapping Core Location Regions (CLR) is tested. The TIET-GEO framework design provides the efficiency to handle multiple geofences and overlapping CLR by notifying the user over email. Let's suppose we are defining a geofence around the United State and a smaller geofence around different states such as New York and Virginia. When the users are entering the United States, the user will trigger the action of entering the United States geofence. When the user moves into New York State the user will trigger into new entering New York geofence, while not leaving the United States geofence.

So, the user has been registering into both geofences, when the user exits from the New York geofence and enters the Washington geofence. In this case, the user will trigger the action of exiting the New York geofence and entering the Washington geofence while not exiting the United States geofence, so by defining the smaller geofence into multiple regions are not registering over a bigger geofence or overlapping region as both geofences are registering with a different unique id and both regions have triggered the action separately. Figure 12 shows the overlapping geofence area.

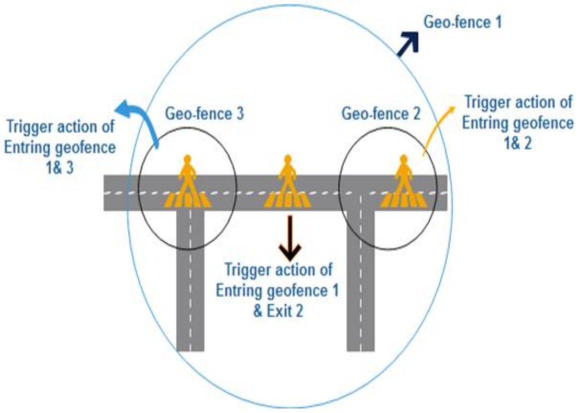
Geo-fence 1
Trigger action of Entring geofence 1& 3
Geo-fence 3
Geo-fence 2
Trigger action of Entring geofence 1& 2
Trigger action of Entring geofence 1 & Exit 2

Figure 12. Overlapping geofence areas demonstration.

Scenario 3: This scenario demonstrated the triggering of the device's action on the boundaries of the geofence area, TIET-GEO also shows successful trigger movement of the devices either inside or outside the bounding area or on the line of the bounding of the geofence area. The haversine formula discusses the triggered action of the device movement by calculating the distance between the points of latitude and longitude in Algorithm (2) and shows the larger distance between the point and trigger action will be outside the bounding geofence area even if the device is moving on the line of bounding area as showing in Figure 13.

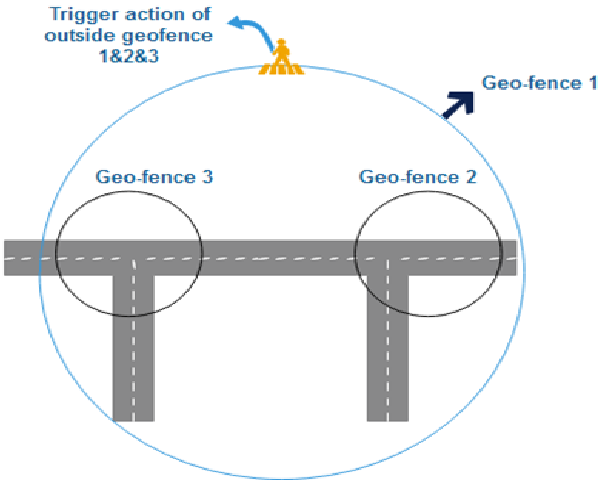

Figure 13. Bounding movement of the geofence.

Scenario 4: This scenario demonstrates the location privacy of device trajectories in real-time from the attackers to extract the user real location user. The dummy location privacy shows the ability to generate numbers of dummy locations based on the size radius of the geofence area in Algorithm (2), where each geofence area will generate a different number of dummy location-based on the size of the radius of the geofence. The minimum number of dummy locations in any geofence area will be based on r/2 of the radius of the geofence area in Algorithm (1), in Figure 14 shows the number of dummy locations in the geofence area.

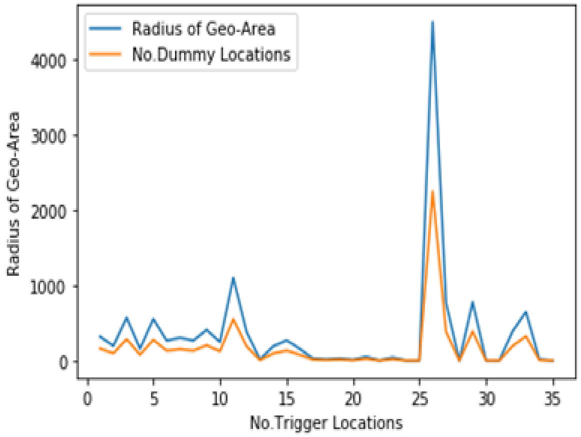

Figure 14. Generate dummy locations based on radius Geo-area.

Scenario 5: In Figure 15 is showing the number of k-dummy location-based on the radius range of the particular geo-area. The k-dummy locations around the user's location will be generated based on two factors: firstly, define the radius of the geo-fence area. Secondly, the number of dummy location-based on the different distances between both locations (real and dummy). The framework shows flexibility and reliability by generating the dummy locations around the user location.

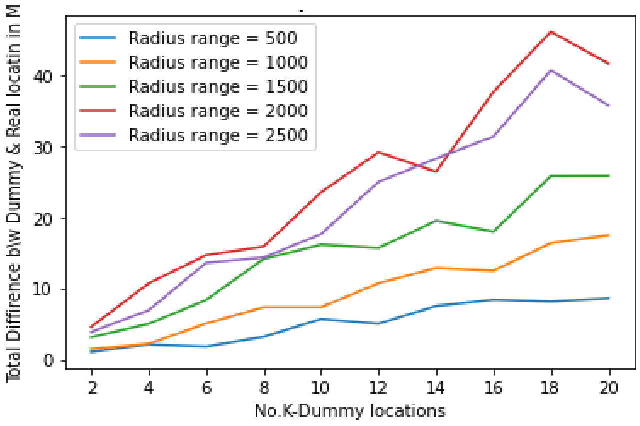

Figure 15. The total distance of the dummy location based on radius Geo-area.

Table 2 discuss the comparison results of the proposed framework with the previously existing method.

Table 2. The comparison results.

Method	Discussion
Overlapping geofence areas demonstration method	The proposed framework TIET-GEO shows the efficiency of responses to different trajectories from different sources of devices such as (mobile, vehicular, and IoT devices). The majority of the proposed method is enhancing the triggers action of user movements into multiples geofences area and provides the location privacy when the user enters or exits the geofence area. The recently proposed novel and mothed only addressed the single trigger geofence area by ignoring the overlapping geofence that occurs as discussed in [5, 9, 16, 17, 20, 34], where the researchers proposed only triggers of user's action within a single geofence area. The researcher in [11, 12] proposed smart notification of accessing multiple geofences of one scenario by moving from one geofence into another, our proposed framework was addressing four scenarios of trigger the users' movements in the geofence area.
Dummy location privacy	Our proposed framework is based on using the dummy mothed to enhance the location privacy of users' trajectories when they enter or exit the particular geofence area. The proposed method will generate a k-dummy location around the user location when they request a POI from the LBS based on the radius of the geofence area. None of the researchers in [5, 11, 16, 20, 21, 34] provide any location privacy of their proposed novel or the methods to secure the user movements or when they request a POI from the LBS services.

6. Conclusions

In this paper, we proposed TIET-GEO which is a geofence service framework for vehicles and users with smartphones or any GPS-equipped devices. It allows the users and trusted third parties to define a geo-area on a map. Corresponding actions are triggered when any device enters or exits a specific geofence area by sending email notifications to users or trusted third parties. Also, we enhanced the location privacy preservation of the users' trajectory movement by using dummy generating methods. Our method provided k numbers of dummy locations around the real user's location within the range of the radius of the circle to ensure the anonymity of the user's location when sending requests to LBS services. Insecurity web services, we introduced token authentication communication using the TIET-GEO framework with the vehicular network when requesting information from the database. The token authentication can verify the users' credentials to provide access to the users into the TIET-GEO service. The proposed framework demonstrated the flexibility of working with different devices and datasets because we tested the framework using different datasets and devices, including android smartphones.

References

[1] Agarwal Y., Jain K., and Karabasoglu O., "Smart Vehicle Monitoring and Assistance Using Cloud Computing in Vehicular Ad Hoc Networks," *The International Journal of Transportation Science and Technology*, vol. 7, no. 1, pp. 60-73, 2018.

[2] Al-Balasmeh H., Singh M., and Singh R., "Framework of Data Privacy Preservation and Location Obfuscation in Vehicular Cloud Networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 5, p. e6682, 2022.

[3] Benarous L., Bitam S., and Mellouk A., "CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7153-7160, 2021.

[4] Benarous L. and Kadri B., "Obfuscation-based Location Privacy-preserving Scheme in Cloud-enabled Internet of Vehicles," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 461-472, 2022.

[5] Cheng G., Guo Y., Chen Y., and Qin Y., "Designating City-wide Collaborative Geofence Sites for Renting and Returning Dock-less Shared Bikes," *IEEE Access*, vol. 7, pp. 35596-35605, 2019.

[6] Cho S. and Kim H., "Privacy Preserving Authenticated Key Agreement Based on Bilinear Pairing for Uhealthcare," *The International Arab Journal of Information Technology*, vol. 18, no. 4, pp. 523-530, 2021.

[7] Durst C., Hacker J., and Berthelmann T., *Digital Customer Experience*, Springer, 2019.

[8] Elazab M., Noureldin A., and Hassanein H., "Integrated Cooperative Localization for Vehicular Networks with Partial GPS Access in Urban Canyons," *Vehicular Communications*, vol. 9, pp. 242-253, 2017.

[9] Garzon S., Arbuzin D., and Küpper A., "Geofence Index: A Performance Estimator for the Reliability of Proactive Location-based Services," *in Proceeding of the 18th IEEE International Conference on Mobile Data Management*, Daejeon, pp. 1-10, 2017.

[10] Greenwald A., Hampel G., Phadke C., and Poosala V., "An Economically Viable Solution to Geofencing for Mass-Market Applications," *Bell Labs Technical Journal*, vol. 16, no. 2, pp. 21-38, 2011.

[11] Guo C., Guo W., Cao G., and Dong H., "A Lane-Level LBS System for Vehicle Network with High-precision BDS/GPS Positioning," *Computational Intelligence and Neuroscience*, vol. 2015, 2015.

[12] Hara T., Suzuki A., Iwata M., Arase Y., and Xie X., "Dummy-Based User Location Anonymization under Real-World Constraints," *IEEE Access*, vol. 4, pp. 673-687, 2016.

[13] Hayashida S., Amagata D., Hara T., and Xie X., "Dummy Generation Based on User-Movement Estimation for Location Privacy Protection," *IEEE Access*, vol. 6, pp. 22958-22969, 2018.

[14] Liu J. and Wang S., "All-Dummy K-Anonymous Privacy Protection Algorithm Based on Location Offset," *Computing*, pp.1-13, 2022.

[15] Lu H., Jensen C., and Yiu M., "Pad: Privacy-area Aware, Dummy-based Location Privacy in

Mobile Services," *in Proceedings of the 7th ACM International Workshop on Data Engineering for Wireless and Mobile Access*, Vancouver Canada, pp. 16-23, 2008.

[16] Nait-Sidi-Moh A., Ait-Cheik-Bihi W., Bakhouya M., Gaber J., and Wack M., "On the Use of Location-Based Services and Geofencing Concepts for Safety and Road Transport Efficiency," *in Proceeding of the International Conference on Mobile Web and Information Systems*, Paphos, pp. 135-144, 2013.

[17] Nardini G., Stea G., and Virdis A., "Geofenced Broadcasts via Centralized Scheduling of Device-to-Device Communications in LTE-Advanced," *in Proceeding of the Workshop on New Frontiers in Quantitative Methods in Informatics*, Venice, pp. 3-17, 2017.

[18] Ni L., Yuan Y., Wang X., Yu J., and Zhang J., "A Privacy Preserving Algorithm Based on R-Constrained Dummy Trajectory in Mobile Social Network," *Procedia Computer Science*, vol. 129, pp. 420-425, 2018.

[19] Niu B., Zhang Z., Li X., and Li H., "Privacy-Area Aware Dummy Generation Algorithms for Location-based Services," *in Proceeding of the IEEE International Conference on Communications*, Sydney, pp. 957-962, 2014.

[20] Oliveira R., Cardoso I., Barbosa J., Da Costa C., and Prado M., "An Intelligent Model for Logistics Management Based on Geofencing Algorithms and RFID Technology," *Expert Systems with Applications*, vol. 42, no. 15-16, pp. 6082-6097, 2015.

[21] Rodriguez Garzon S. and Deva B., "Geofencing 2.0: Taking Location-based Notifications to the Next Level," *in Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, Seattle, pp. 921-932, 2014.

[22] Skala V. and Majdisova Z., "Fast Algorithm for Finding Maximum Distance with Space Subdivision in E 2," *in Proceeding of the International Conference on Image and Graphics*, Tianjin, pp. 261-274, 2015.

[23] "The PHP Framework for Web Artisans," (n.d.), Laravel, https://laravel.com/, Last Visited, 2022.

[24] "UCI Machine Learning Repository: Bike Sharing Dataset Data Set," (n.d.)). UCI Dataset Repository, Retrieved, https://archive.ics.uci.edu/ml/datasets/bike+sharing+dataset, Last Visited, 2022.

[25] "UCI Machine Learning Repository: GPS Trajectories Data Set," (n.d.). UCI Dataset Repository, Retrieved from https://archive.ics.uci.edu/ml/datasets/GPS%20Trajectories, Last Visited, 2022.

[26] Ullah I., Shah M., Khan A., and Jeon G., "Privacy-preserving Multilevel Obfuscation Scheme for Vehicular Network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, pp. e4204, 2021.

[27] Wang T., Zeng J., Bhuiyan M., Tian H., Cai Y., Chen Y., and Zhong B., "Trajectory Privacy Preservation Based on A Fog Structure for Cloud Location Services," *IEEE Access*, vol. 5, pp. 7692-7701, 2017.

[28] Wu D., Zhang Y., and Liu Y., "Dummy Location Selection Scheme for K-Anonymity in Location Based Services," *in Proceeding of the IEEE Trustcom/BigDataSE/ICESS*, Sydney, pp. 441-448, 2017.

[29] Wu X. and Sun G., "A Novel Dummy-based Mechanism to Protect Privacy on Trajectories," *in Proceeding of the IEEE International Conference on Data Mining Workshop*, Shenzhen, pp. 1120-1125, 2014.

[30] Wu Z., Li G., Shen S., Lian X., Chen E., and Xu G., "Constructing Dummy Query Sequences To Protect Location Privacy and Query Privacy in Location-Based Services," *World Wide Web*, vol. 24, no. 1, pp. 25-49, 2021.

[31] Yim Y., Cho H., Kim S., Lee E., and Gerla M., "Vehicle Location Service Scheme Based on Road Map in Vehicular Sensor Networks," *Computer Networks*, vol. 127, pp. 138-150, 2017.

[32] Yu H., Li G., Wu J., Ren X., and Cao J., "A Location-based Path Privacy Protection Scheme in Internet of Vehicles," *in Proceeding of the IEEE INFOCOM-IEEE Conference on Computer Communications Workshops*, Toronto, pp. 665-670, 2020.

[33] Zheng Y., Fu H., Xie X., Ma W., and Li Q., "Geolife GPS Trajectory Dataset-user Guide-Microsoft Research," 2011.

[34] Zhou Z., Yu F., and Shang J., "iGeoNoti: A Fine-Grained Indoor Geo-notification System," *in Proceeding of the 4th International Conference on Ubiquitous Positioning, Indoor Navigation and Location Based Services*, Shanghai, pp. 192-196, 2016.

Hani Al-Balasmeh is a PhD student in the Computer Engineering Department at the Thapar Institute of Engineering & Technology in Patiala, India. He recently received his M.Sc. in Information Technology from the University of Mysore with (Distinction) in India. His research interest is in vehicular cloud networks, data & location privacy, and IoT.

Maninder Singh is Ph.D. in Computer Science with specialization in Network Security and M.E. in Software Engineering from Thapar Institute of Engineering and Technology, Patiala and B.E. in Computer Engineering. He joined the Computer Science and Engineering Department of Thapar Institute of Engineering & Technology, Patiala (India) in 1996 and is presently serving as professor and dean of Academic Affairs. His research interests include Network Security, Cyber Physical Systems & Security and IoT.

Raman Singh, is a Lecturer in the School of Computing, Engineering, and Physical Sciences, the University of the West of Scotland, Lanarkshire, United Kingdom. I have worked as a Postdoctoral Fellow at the School of Computer Science and Statistics, Trinity College Dublin, The University of Dublin, Ireland from February 2020 to February 2021. I also worked as an Assistant Professor in the Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala (India) from June 2016 to November 2021. My primary research interest is in the area of cyber and network security. I have completed a Post-Doc Fellowship in Blockchain and Applied Cryptography and a Ph.D. in Machine learning-enabled Intrusion Detection systems.