IDP: A Privacy Provisioning Framework for TIP Attributes in Trusted Third Party-based Location-based Services Systems

Muhammad Usman Ashraf[1]
Department of Computer Science
University of Management and
Technology, Sialkot, Pakistan

Kamal M. Jambi[2]
Department of Computer Science
King Abdulaziz University
Jeddah, Saudi Arabia

Rida Qayyum[3], Hina Ejaz[4]
Iqra Ilyas[5]
Department of Computer Science
Govt. College Women University
Sialkot, Pakistan

***Abstract*—Location-Based Services (LBS) System is rapidly growing due to radio communication services with wireless mobile devices having a positioning component in it. LBS System offers location-based services by knowing the actual user position. A mobile user uses LBS to access services relevant to their locations. In order to provide Point of Interest (POI), LBS confronts numerous privacy related challenges in three different formats including Non-Trusted Third Party (NTTP), Trusted Third Party (TTP), and Mobile Peer-to-Peer (P2P). The current study emphasized the TTP based LBS system where the Location server does not provide full privacy to mobile users. In TTP based LBS system, a user's privacy is concerned with personal identity, location information, and time information. In order to accomplish privacy under these concerns, state-of-the-art existing mechanisms have been reviewed. Hence, the aim to provide a promising roadmap to research and development communities for the right selection of privacy approach has achieved by conducting a comparative survey of the TTP based approaches. Leading to these privacy attributes, the current study addressed the privacy challenge by proposing a new privacy protection model named "Improved Dummy Position" (IDP) that protects TIP (Time, Identity, and Position) attributes under TTP LBS System. In order to validate the privacy level, a comparative analysis has been conducted by implementing the proposed IDP model in the simulation tool, Riverbed Modeler academic edition. The different scenarios of changing query transferring rate evaluate the performance of the proposed model. Simulation results demonstrate that our IDP could be considered as a promising model to protect user's TIP attributes in a TTP based LBS system due to better performance and improved privacy level. Further, the proposed model extensively compared with the existing work.**

Keywords—Location Based Services (LBS); Trusted Third Party (TTP); privacy protection goals; mobile user privacy; Improved Dummy Position (IDP); Sybil Query

I. Introduction

In recent years, location-based services (LBS) gaining popularity due to the rapid advancement of mobile phones, wireless communication, and positioning systems among users [1]. In Location-based services, the mobile user can get his/her current location from GPS available in their mobile phone, posting a query for services to LBS System that contains his actual location. LBS returns point of interest (POI) to a user based on his/her request. It can be used to trace the nearest cinema, restaurant, hospital, or desired destination from your location according to the shortest route. Some examples of such requests include points of interest (POI) queries, for example, "Which Chinese food restaurant is near to my current location?" queries of real-time traffic, "How swarming is the way from my house to my office?" [2], and data processing over Fog [63], cloud [64].

The essential origin of the LBS system was the Enhanced E911 authorization, passed in 1996 by the government of the U.S [29]. This authorization for operators of the mobile network distinguish emergency callers with efficiency, so the location of the caller is distributing to public safety answering points. Cellular machinery could not fulfill these certainty needs, so the operators started excessive effort to introduce advanced positioning methods. Operators launched a sequence of LBSs commercial to gain a return on Enhanced 911 investments. In many cases, on request, these comprised of services that send to users a set of Point-of-Interest (POI) such as gas station, shopping mall, coffee shop, in recommender systems [62] ATM, hospitals, and clinics. After all, many users have not to seem involved in this type of LBS system that is why most operators immediately abolish their LBS contributions and cancelled relevant evolution attempts [30].

The first web-based mobile device released in 1999 has the capability of LBS named the Palm VII. TeliaSonera in Sweden (Friend Finder, house position, emergency call location) introduce the first LBS in 2001. Further, go2 with American Telephone and Telegraph Mobility in May 2002 began the first United States application of mobile local search that used Automatic Location Identification (ALI) technologies [31]. Senator Al Franken introduces the Location Privacy-Preserving Act of 2012 to modulate the transmission and distribution of user location information in the United States (US). Till 2005, the major challenge of privacy was addressed by the TTP. Later on, NTTP in LBS was introduced, and still further work and research is required to provide sufficient privacy using these two ways in LBS System.

In the LBS system, there are three technologies used in a single device: internet access in mobile, positioning component, and user-friendly interfaces. In the late 1990's mobile phones availability only provides the facility of voice and SMS. There was a lack of user interface facilities. Whereas these technologies already utilize LBS systems. After the addition of Wireless Application Protocol (WAP) and mobile phone internet, the news was, announced about the availability of general LBS Systems [32].

The primary components of an LBS System [3] are end user's Mobile devices (e.g., smartphones), Communication network to send queries and receive services, Software application presents the services, Services provider that provide requested services to end-user and a positioning component to locate the position of the user like Global Positioning System (GPS). The LBS system provides useful and suitable location information to LBS users. When a user requests for the services from the LBS system [33] concurrently, they must reveal their location information. At that time, their personal information is at a risk. With the tremendous growth of LBS services, it is a great challenge to provide useful services under a fully private environment. Fig. 1 illustrates the fundamental LBS architecture.

Conventionally, the LBS system is used in three basic categories such as Non-Trusted Third Party (NTTP), Trusted Third Party (TTP), and Mobile Peer-to-Peer based network (P2P) [4]. All these models are composed of three components as User Mobile device, Location Server, and client. The primary objective is to provide desired services or Point-of-Interest (POI) to each client interacting or making a request to the LBS system. In order to retrieve the results, the Location Server (LS) further communicates with clients to acquire the requested location. Fig. 2(a), illustrates the Non-Trusted Third Party (NTTP) model [5] where no third party involved for preserving privacy. Its minor part based on silent period, Coordinate transformation, the L4NE protocol [6], [8], Decentralization [7], [9], Cache Based Approach [11], [13], Optimal Mechanism [10], [12], Geo Indistinguishability [14], Context-Aware Privacy Protection (CAP) [15], [17], HBLP [61] and blind filtering [16] are the examples of NTTP schemes. Further, Fig. 2(b), shows the Trusted Third Party (TTP) model using an anonymizer that guarantees reliability in order to deal with k-anonymity [18], [20], mix zone [21], dummy position models [19], [22]. Further, the third category mobile Peer-to-Peer based network (P2P) presented in Fig. 2(c) where, there is no secure transmission infrastructure, client-server, and centralized/distributed architecture. Every mobile user device interacts with another mobile user for the desired location or Point-of-interest (POI) [23].

In the TTP LBS system, the Service provider is unaware of real user identity and its current location [24]. However, TTP guarantees the privacy of the mobile user using the LBS system. In our study, the main concern is to provide privacy to mobile user personal information such as his identity, spatial and temporal information in TTP Based LBS systems so that mobile users safely communicate and no one misuse their private information while accessing services [25]. For this reason, the main objective is to protect the location information and make it impractical to figure out it from many traces. However, a new privacy approach is proposed that will protect Time, Identity, and Position matrices for TTP Based LBS system. Fig. 3 comprises mobile user, communication network, positioning technology, anonymizer, service provider, and content provider.

The primary objective of the current study was to provide privacy to the mobile user in the TTP based LBS systems. Based on fundamental privacy attributes discussed in section 2, we have enhanced the "Position Dummy" model with new mechanisms to achieve our research objectives. Therefore, we have proposed a new privacy provisioning model named Improved Dummy Position (IDP). The results of this work expected to provide a proper environment to the LBS system and reduce the privacy issues between the user and Location Server (LS). However, the contribution of this paper can be summarized as follows.

- We propose an IDP System model for TTP based LBS system by extending the base Dummy Position technique, which resolves the privacy problems of the user regarding the disclosure of personal information.
- We evaluated the effectiveness of the proposed model by presenting an Improved Dummy Position (IDP) algorithm.
- In order to make sure the privacy authenticity, we implemented the proposed model in real France highway road networks using Riverbed modeler academic edition 17.5 simulation tool and measured different privacy factors including Ethernet delay, Query success rate, system performance with load and query processing time, route API retransmission and data access rate.

Further, the proposed model extensively compared with the existing work. It was observed that IDP outperformed the existing state-of-the-art models.

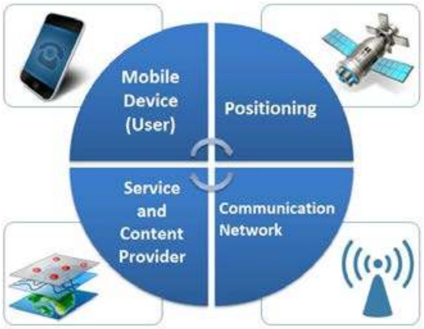
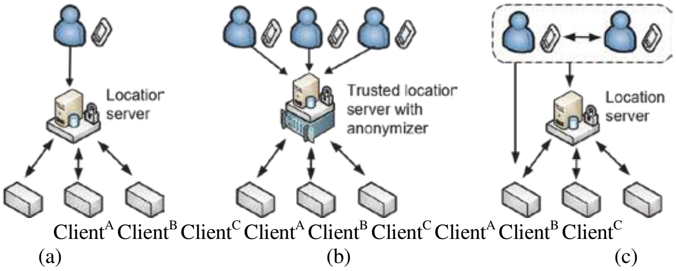


Fig. 1. A Common LBS Architecture.


Location server
Trusted location server with anonymizer
Location server
Client^{A} Client^{B} Client^{C} Client^{A} Client^{B} Client^{C} Client^{A} Client^{B} Client^{C}
(a)
(b)
(c)

(a) Non-trusted third party. (b) Trusted third party with anonymizer. (c) Mobile peer-to-peer network.

Fig. 2. Standard LBS Models.

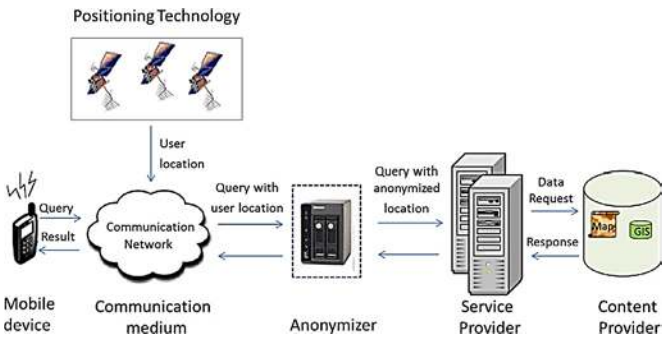


Fig. 3. An Overview of TTP LBS System.

The rest of the paper is structured as follows. Section II highlights the privacy challenges and protection goals of the TTP based LBS system. A comprehensive literature on TTP LBS models is presented in Section III. Section IV demonstrates the motivation toward the IDP system model, algorithm design, and its framework. Section V presents the experimental evaluation of the IDP scheme using simulations. Section VI highlighted the discussion. Finally, we conclude this paper and outline future work in Section VII.

II. Privacy Challenges and Protection Goals in LBS System

LBS system usage is rapidly growing nowadays but its extensive use raises many affairs. Still, LBS service providers are reluctant to build a proper environment in which they don't have an approach to user's personal information. Consciously or unconsciously, most users are ready to give one or more pieces of their personal information in order to gain new services [26], [27], [59]. User information received and saved in the LBS server can reveal extremely private information. For instance, where a user goes, whom they see, and what they do. Failing to keep this information private may threaten privacy rights. LBS server may access the user location information, which may disturb the user like the privacy of the LBS user, location information certainty, pricing, availability of data, etc. Among these challenges, "Privacy" is the critical one while using the LBS system. When a user posted a query to LBS, they send their location and related personal information to Location Server. At that time, their privacy is at the risk. These issues while using TTP Based LBS System end up with the disclosure of LBS user time of the query, their personal information (Identity), and location-related information. Therefore, these TIP (Time, Identity, Position) attributes of the LBS user need to be protected. A distinct defense against privacy issues is to exclude any data from the request that can precisely confess the LBS user identity, it is possible by using a pseudonym whenever it is needed.

In LBS System, three privacy metrics are needed to be preserved in order to provide a fully protected environment to the mobile user [25] [60]. These attributes include the user's identity, user's spatial information, and temporal information as shown in Fig. 4. The privacy of user identity means that a malicious party is unable to infer the information about the user from the previous activities. Whereas, spatial information refers to location information that puts the privacy of the user at risk. Moreover, the privacy of temporal information is to hide the time of the query from an attacker so that from time factor actual location of the user could not be disclosed. The protection of stated attributes describes the research objective which is addressed in the current study.

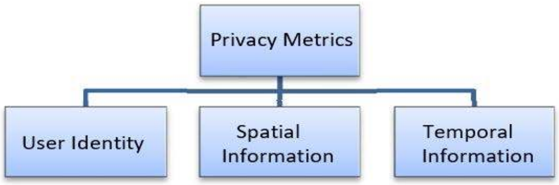


Fig. 4. LBS Privacy Metrics.

A. *UserIdentity*

The purpose is to obscure the identity of the mobile user while making a query to the LBS System so that the attacker could not reveal their identity. The identity can be a name, an ID, or any aggregation of the related key terms that are used to uniquely identify the user [28]. The disclosure of user identity can put the privacy of LBS users at risk therefore, it is necessary to preserve mobile user identity in order to save LBS users from information leakage.

B. *Spatial Information*

Another protection goal is to hide the user's actual position form the attacker. When the user makes a query to LBS they have to send their current location information to Location Server, the adversary could hack this information to locate the user and use this for the wrong purpose. Therefore, disclosing spatial information puts user privacy at risk. For instance, a person who wants to visit the nearest cafe posted a query "What is the nearest cafe from my current location". Meanwhile, to get the service he has to send his current actual position. Therefore, the privacy of spatial information is necessary for the LBS user.

C. *Temporal Information*

The intention is to hide the time information of the posted query to the LBS system. This is the time when a user making a request to LBS and sent their personal information and actual location. Therefore, the exposure of temporal information damages the user's privacy by disclosing their identity and locating his accurate position [28]. That is why the protection of temporal information is needed to provide full privacy to LBS users.

In order to achieve these three privacy metrics, there is need to depend on Trusted Third Party (TTP) where LBS System protect the information about the mobile user such as where they live, where they work and thus makes it impossible for an adversary to track the user and misuse their personal information.

III. Related Work

In order to protect a user's privacy in an LBS system, several approaches have been proposed. In this section, we have reviewed several Trusted Third Party (TTP) based techniques to preserve the privacy of the LBS user.

Location cloaking [34] mechanism uses the anonymizer (Trusted Third Party) where the cloaking region is created, and the position of a user and other k-1 neighbors kept in it. Such type of architecture is 3-tier architecture as shown in the figure below. Such type of anonymizer protects the user's identity and spatial information. The idea of K-anonymity approaches relies on the location clocking approach where the TTP LBS user's location is hiding among K-1 neighbours. Fig. 5, depicts the Location cloaking using anonymizer between user and location server. Permanent conversation and remote checking of the user is required to let the anonymizer frequently update the current position of all the subscribed users of LBS, which is the violation of the users' privacy.

Gruteser and Grunwald [35] present the concept of the K-anonymity technique. In this approach, the TTP LBS user accommodates his true position and the position of other k-1 users decides an obfuscation region. At this moment, Location Server (LS) acts as a trustworthy entity that calculates the obfuscation area that contains a mobile user's position and a set of other k users. This technique greatly protects the user's identity by a pseudonym, but it does not implement satisfactory protection across attribute disclosure.

In order to preserve the LBS user privacy, there are further approaches that are based on the concept of the k-anonymity [36]. These are strong k-anonymity, l-diversity, t-closeness, p sensitivity, historical k-anonymity. According to the Clique Cloak technique [37], [38] proposed by Gedik et al. The privacy level of k-Anonymity and some of its enhancements is to protect the user's identity and spatial information of the mobile user.

Zhang et al. [39] proposed a strong k-anonymity technique. In this technique over multiple queries, the same cluster of k users is calculated. Therefore, the attacker who calculates different clusters to infer TTP LBS users cannot identify a user. By using the concept of generalization and suppression strong k-anonymity is attaining the least misinterpret outcomes. Strong k-anonymity is not always satisfied by generalization even though all Data fly generalizations do satisfy k-anonymity. For making this heuristic-based approach more work is required.

Bamba et al. proposed the concept of l-diversity [40]. This approach ensures that the TTP LBS user's position is identical and the position of k users is evenly scattered at a certain distance from each other's. The sensitivity level of each attribute is high in this technique. Therefore, it desires much effort to achieve privacy for LBS users. L-diversity solves attribute disclosure problem that is available in k-anonymity. But l-diversity may be unnecessary to achieve. Fig. 6 illustrate the privacy provision by k-anonymity and l-diversity.

The perception of t-closeness suggested by Li et al. [41], enlarges the concept of l-diversity. It assures the distance between the distribution of sensitive attributes and the distribution of attributes within the k user's cluster. This area should not be lesser than a threshold. T-closeness can be applied using distance measures like Earthmover's distance (EMD).

Domingo-Ferrer et al presented the concept of p-sensitivity [42]. Its concept is that there are different values of p for each confidential attribute sharing a mixture of key attributes within the record. It protects from location attack by de-linking each user query from his generator, which distracts the attacker that there are several users available in a particular clocking region (CR). It provides an efficient way to determine the sensitivity of parameters with respect to the output. Information loss is higher when p-sensitive is enforced on a dataset compared to when the dataset is masked according to k-anonymity only.

Mascetti et al. [43] guarantee historical k-anonymity, which expands the concept of k-anonymity for moving objects. From Fig. 7, it is clear that the user is continuously moving from one place to another. In this approach, the system holds the record of each user movement, his history, and for creating the anonymity area main this moment history information. Hence, this anonymity area is sent to the TTP LBS system to gain the services against the request. Therefore, this is a convenient approach for preserving user position using the k-anonymity framework.

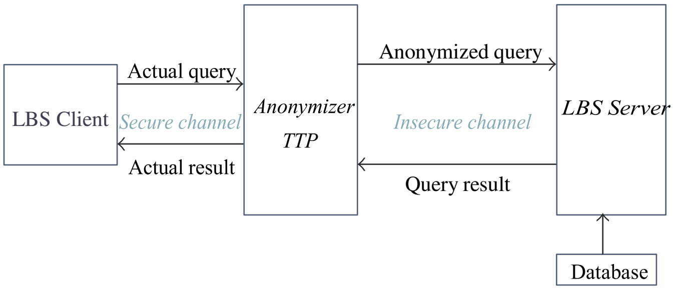


Fig. 5. Location Cloaking using Anonymizer between LBS user and Location Server.

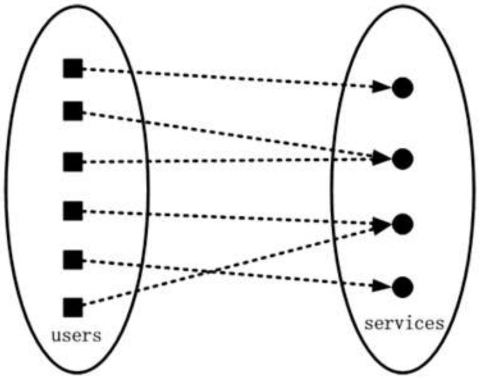


Fig. 6. Privacy Provision by K-Anonymity and l-Diversity.

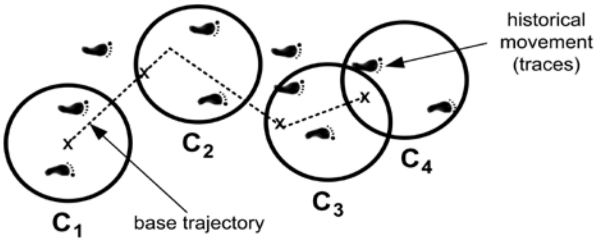


Fig. 7. K-Anonymity based on Historical Movement.

Kido et al. [44], [49] proposed the Position dummies technique which is considered as one of the reliable approaches for location protection. The main principle of the dummy position approach is defined as mobile users dispatch their current position along with multiple fake locations where mobile users' precise information is identical, thus posting a query to Location Server (LS) [50]. But at the same time it is a challenge to create non-distinguished dummies from the actual user position. In particular, if an attacker is able to track the user for a longer time and has context information about the user. When TTP LBS user changes his position and moves from X to Y, he posts a new request by sending his actual location along with new multiple false dummies according to new event or destination as shown in Fig. 8.

The advanced method to generate dummies is Sybil Query presented by Shankar et al [45]. It is a client-side tool where a user has a historic traffic database that allows them to generate multiple distinguishable dummies for the mobile user. For example, a Mobile user request for a TTP LBS server for a busy downtown area. Sybil queries will generate dummies that are from the related traffic area and conditions. Sybil Query delivers these queries to the TTP LBS system, which is incapable to differentiate the actual query from the synthetic queries [51].

Beresford presents a novel approach as "Mix Zone" for location privacy protection [46]. The fundamental concept of this technique was to hide the mobile user's actual location in a special region where others do not know that users position; an attacker could not identify who is continuously posting queries to TTP Based LBS System. In this way, TTP LBS user identity and spatial information have preserved under this mechanism. Mix zones are replacing the concept of the Spatial Cloaking technique and provide protection against location privacy. Existing mix-zone ideas fail to provide impressive mix zone construction algorithms that are effective for mobile users moving on road networks.

Palanisamy and Liu. [47] Proposed MobiMix approach. Its concept follows the mix zone technique where an attacker could exploit the personal detail such as TTP LBS user's identity, temporal and spatial information by analysis, and take full advantage largely. It is possible due to the timing of the mobile user when he enters in zone A and exit from zone A to zone B. This assist the attacker to easily identify the new and old pseudonyms.

Jiang et al. [48] proposed policy-based schemes. Policies are the statements, which determine what service provider can do with the Mobile users' private information. These policies are issued by the Service provider. If the provider does not follow these policies, then the user has the right to take legal action against the service provider. TTP LBS user has numerous policies, it's up to the user's hand to control what data is collected and with whom it would be shared. To choose policy among a number of policies, choose a policy that saves money and does not expose a user's personal data to the third person but as response service providers can hand over the user data to others in exchange for money.

Pseudonymisers [48] is a trusted third party, which acts as an intermediate among service providers and mobile users. It receives a request from the user, replaces actual user IDs with the fake ones, and sends it to the service provider. Therefore, the service provider does not know the real ID of the LBS user because it remains private. In this technique user, fully trust on it that is why Real IDs and related pseudonyms are stored in Pseudonymisers and t sent to the system to gain the services for the user, but the service provider could infer the real identity of the LBS user by linking the locations of the user.

Route Server [4] preserve the mobile user's identity and spatial information by providing accurate and efficient results for requests. To post a route request there are queries of Q set q1, q2, q3 . . . Qn, at this junction each query (q) belongs to set Q, it allows an adversary to generate some wrong information by acknowledging the user's actual location information. The challenge was provisioning privacy to the mobile users from an attacker who will conclude the wrong data in actual data when the LBS user posted a query to the system [52].To improve privacy, the Route Server (RS) algorithm has proposed a new authentic approach/technique, which is AES-RS architecture.

AES-RS architecture [4] is the enhancement of the Route Server (RS) algorithm. In this architecture, the idea of a dummy position is used where a number of dummy (fake) positions are generated along with a single user request. This architecture mainly preserves the TTP LBS users' identity and actual location from the attacker. The mechanism of this architecture is that mobile users and dummies send to the TTP LBS System, which further finds out the Point of Interest (POI) from either Route Log "L" or Road Networks "G". Based on AESRS architecture, Dummy Data Array (DDA) Algorithm is designed which is more efficient in performance [56] [58].

Based on privacy protection goals discussed in the previous section, we have conducted a critical analysis in this study and compared the different state-of-the-art approaches with TIP attributes in Table I as follows.

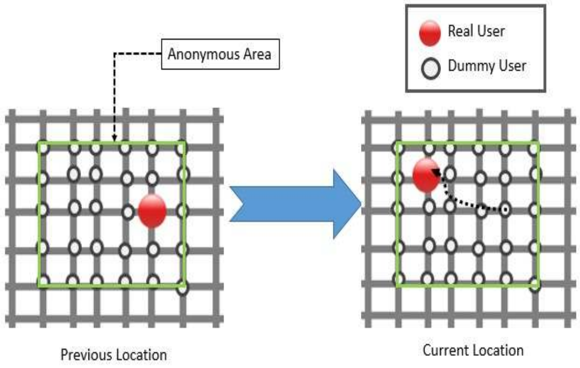


Fig. 8. Dummies on Changing Position.

TABLE I. PRIVACY PROTECTION GOALS IN LBS SYSTEM

Ref. No	Privacy Protection Goals		
	Identity	*Spatial*	*Temporal*
[34]	✓	✓	×
[35]	✓	×	×
[39]	✓	×	×
[40]	✓	✓	×
[41]	✓	✓	×
[42]	✓	✓	×
[43]	✓	✓	×
[44]	✓	✓	×
[46]	✓	✓	×
[47]	✓	✓	×
[48]	✓	✓	×
[48]	×	✓	×
[4]	✓	✓	×
[4]	✓	✓	×

IV. PROPOSED IDP MODEL

This section presents the proposed Improved Dummy Position (IDP) model as shown in Fig. 9, where actual user desire for a point-to-interest to find out the nearby Coffee Shop from his current location using over the road network. Hence, TTP LBS user posted a query to LBS System in order to find out a route path or POI (in our scenario "the nearest Coffee Shop"). Here, the LBS System is Trusted Third Party (TTP). When the user is posting a query, at that time their privacy is at risk. In order to overcome these privacy issues and to keep safe their exact location, the IDP mechanism generates dummy positions in a specific area. This area can be in the form of a grid or a circle. Within one of the defined areas, LBS user posted a request with multiple dummies to TTP LBS for the desired event or Point-of-Interest (POI). This proposed model processes that request, search out the required results from Route Log, if found then return the required requested outcomes to TTP LBS user otherwise invoke Route API for the latest results. By posting multiple queries several times (5-10), an attacker can easily identify the actual user and can take advantage of their information.

In order to overcome this problem, whenever the actual user posted a query to the LBS System their identity will be change. In TTP Based LBS System, the Identity is randomly generated unique ID, provided by an additional resource key Generator. Moreover, to generate indistinguishable dummies, it has used one of the advance methods i.e. Sybil Query to generate multiple false locations that resemble the client actual location. Based on this mechanism, it has achieved our protection goals i.e. provisioning privacy to Time, Identity and Position attributes in TTP Based LBS system. Leading to objectives, a proper environment has provided to the LBS system and the privacy issues between the user and Location Server (LS) thus reduced.

Fig. 9 depict three main components of the IDP system model including LBS client, User Dummy Mixer (UDM), and LBS. These components bring a complete architecture to provide a safe environment for the LBS system. The first and foremost component is LBS client that uses the LBS for nearest places from their current location. An additional resource has provided to the LBS client that generates unique random IDs. Key Generator provides every time a unique ID to TTP LBS user when they send a request to LBS for any POI or desired location. In order to generate several dummies that resemble the LBS client's actual location, Sybil Query has been used for this purpose, as it is the most advanced method to produce fake locations. The second component is User Dummy Mixer (UDM) where mobile users' actual position blend with the number of dummies that are undistinguished.

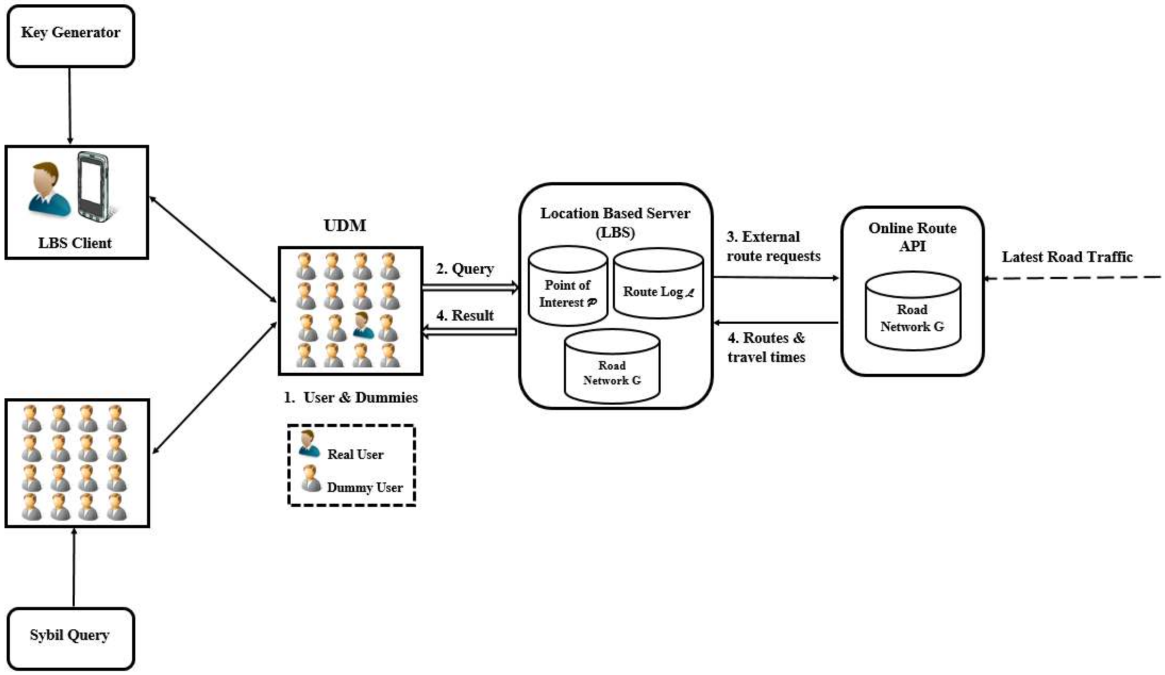


Fig. 9. IDP System Model.

The third and most important component LBS, defined as services accommodate a mobile device location with other information. LBS provides any location-related information according to the desire location that the user has requested to the system. LBS is very useful for users nowadays that it can save a lot of user's time to reach from one location to another. It contains point-of-interest (POI) that users found interest or useful, stores the concurrent POI they have visited frequently. Route log in LBS provide functionalities in the mobile network, which transfer service request such as measuring positions, searching for a route, search to the service provider, search from the service provider based on the user's position. In LBS, the Road network processes the live queries of the mobile user. Online Route API plays a vital role in case if the system does not contain results related to a user's particular request.

A. *Algorithm Design*

Based on the proposed model, we have designed the Improved Dummy Position (IDP) algorithm which is described in Algorithm 1. Note that the same procedure is repeated every time for each user-posted query to TTP Based LBS System. By this algorithm, before sending a request to the LBS system.

- Determine the Anonymity Area A (line 1-3): If the area is grid G, measure the lower limit (L), and upper limit (U), height and width of the distinct space define a grid. To make partition of the grid into the numbers of cells (C) as shown in Fig. 10 L, U coordinates are determined. Each cell Edges (E) and Vertices (V) belong to C, which associated a collection of Edges E, and Vertices V. Vertices are determined besides all cell and one location of the cell given to the user real location.
- In case, the Anonymity Area A is the circle (line 4-5): Angle and radius will measure by respective formulas in order to define an area for user location U(X, Y).
- Set random id provided by the key generator to user location (line 6-8): Assigning the user current location Px, Py to one random cell of gird area G.
- Declare 2-D array DumArr [Nx][Ny], x, y, N, and counter variables i, j (line 9-17): Array consists of a number of N dummies and the index of the user location U(X, Y). A nested while loop is executed to fill the array with dummy positions.
- Add (line 18-19): User current location Px, Py to array and return DumArr[K(x, y) + U(X, Y)].

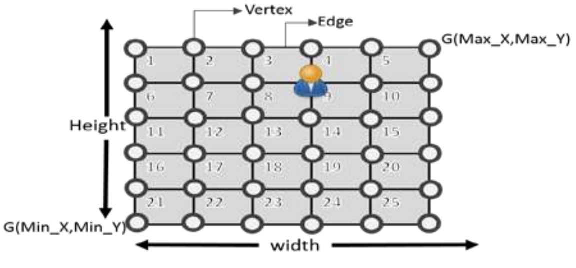


Fig. 10. Grid Partition into Cells.

Algorithm 1: IDP (Improved Dummy Position)

Input: User Location U (X, Y), Anonymous_Area A, Anonymity_Number K, Dummies N, π.

Output: DumArr[K(x,y) + U(X,Y)]

Procedure:

```
1: If(A==G(L, U)) \\ If area is rectangular than calculate both Height and Width, U,L limit.
2: N ← $\sqrt{G}$ \\ Calculate Number of cells in G
3: (V,E) $\in$ N \\ Determine vertices and edges of each cell.
4: Else if (A=Circle(π))
5: $\theta = \frac{2\pi}{k}$; $r = \sqrt{\frac{A}{\pi}}$ ; \\ Calculate both angle and radius
6: U(X, Y) ← Key Generator \\ Determine actual user key
7: Px ← Random (0, v(N-1))
8: Py= ← Random (0, v(N-1))
9: DumArr[$N_x$][$N_y$] \\ Initialize 2-D array
10: i, j, x, y, N \\ Declare variables x-axis, y-axis
11: While (i < N) \\ Fill array with dummy positions
12:             While (j < N)
13:                 DumArr[i][j] ← Sybil Query
14:             j ++;
15:             end loop
16: i ++;
17:       end loop
18: add Px,Py in DumArr
19: Return DumArr
```

Fig. 11 illustrate the proposed privacy-preserving framework for TTP Based LBS System. According to the given algorithm, it takes U(X, Y), A, N, and π parameters as an input. If the anonymity area is Grid G, calculate Lower and Upper Limit (L, U) otherwise, the defined area will be a circle, measure angle, and radius for anonymity area A. The key generator provides a unique ID to actual user U(X, Y). After this, multiple dummy positions generated by Sybil Query. A 2D array initializes in order to store the dummies N in it. The nested loop has executed until the Dummies N filled in an array. Finally, the query has posted to the TTP LBS; system processes it and returns the point of interest (POI) according to request.

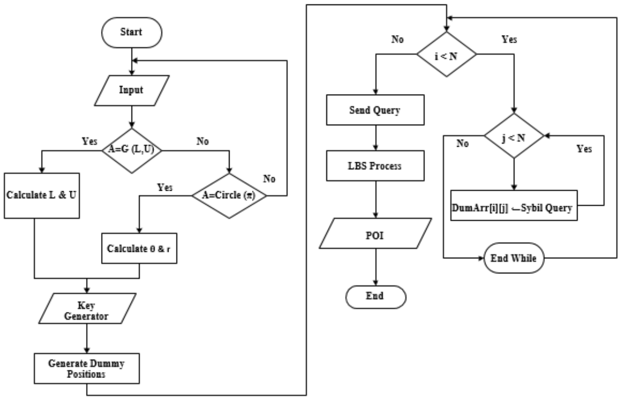


Fig. 11. The Framework of IDP Algorithm.

V. Performance Analysis

In order to evaluate the effectiveness of the proposed Improved Dummy Position (IDP) model, extensive simulation has conducted. In this section, we first describe the simulation environment and present the simulation results. After this, the comparison is performed with Data Dummy Array (DDA) Algorithm.

A. Simulation Setup

In this section, we authenticate the performance of the proposed model with the privacy factors. For this purpose, Riverbed Modeler academic edition 17.5 [53] simulation tool was used. Since it could be used for composing complicated network topologies to simulate the sending/receiving message rate. OPNet Modeler was its old name [54].

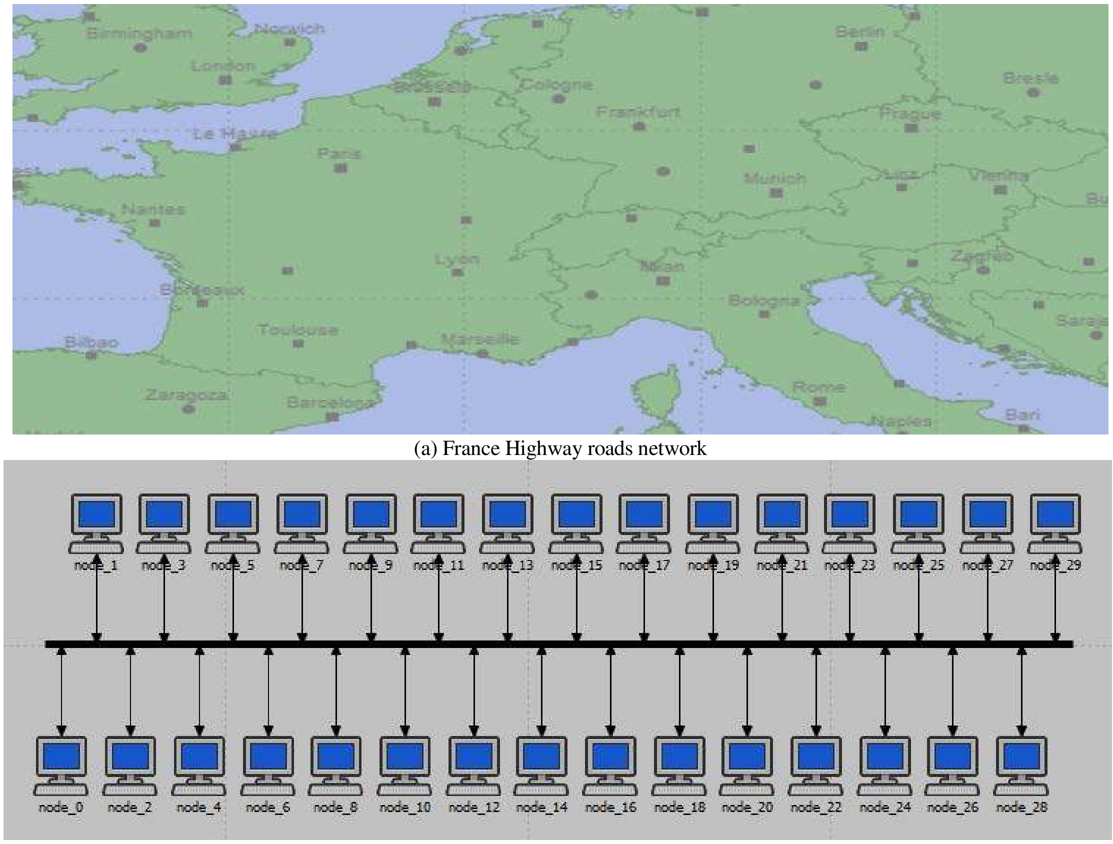
In this simulation, we choose various nodes that represent actual user location from where they want to search out the nearest route path to Coffee Shop in order to preserve personal information of a user along with generated Dummy positions, send to location server over a wireless network. When numerous queries posted to the LBS system and it acknowledges back with a request, the result was evaluated by setting the duration of 1 week. Consider that there is an area A of size 200mx100m. For this simulation, Ethernet and bus topology is constructed. 30 dummy positions/nodes from multiple positions are linked with each other illustrated in Fig. 12(a), (b) and it sends user requests to the TTP LBS system for services. Fig. 13 shows the attributes set during the rapid configuration of bus topology in which value is assigned to a model, delay, and thickness attributes while the rest of the parameters remain default. For nodes, expand the traffic and packet generation arguments where the value of Packet size and Inter arrival Time is modified.

B. Experimental Results

Fig. 14 illuminates the frequency at which LBS receives the data packets which is sent from the Ethernet. We observe that as the time duration increases, the data sending rate (shown in blue line) continual initially but increasing after reaching the maximum. Meanwhile, the query receiving traffic (shown in red line) tends to persistent initially but increasing after reaching the maximum. Further, we observe that it is quite satisfactory for LBS users to take location related services without compromising privacy. The delay in transferring data packets to LBS server were calculated by using “Little’s theorem”.

$$N(t) = A(t) + B(t) \text{ and } t \geq 0 \quad (1)$$

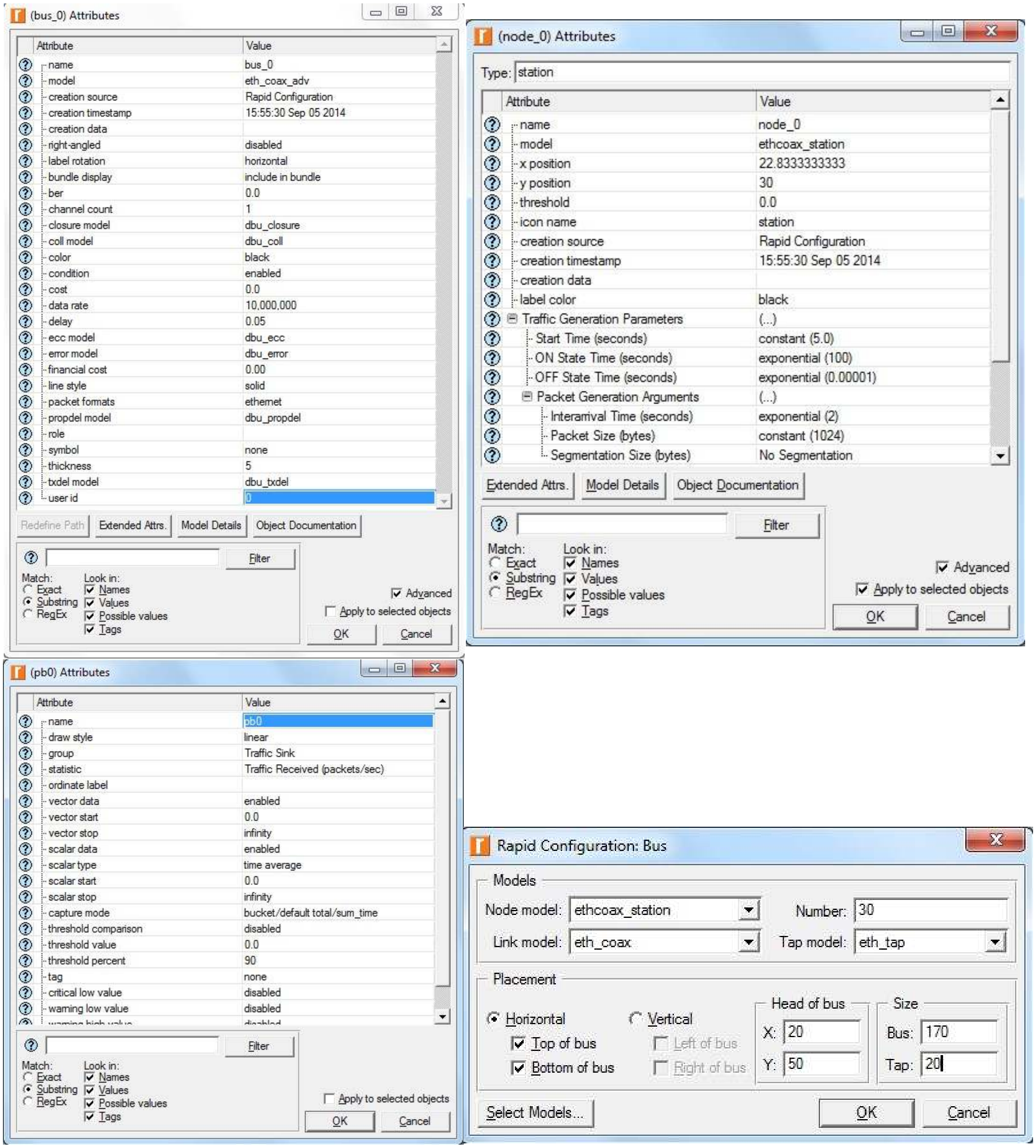
Where A (t) is the number of data packets which are arrived at in time (0, t) and B (t) is the number of data packets that are depart from source location in time (0, t).



(a) France Highway roads network

(b) Simulation Environment

Fig. 12. Riverbed Modeler (OPNet Modeler).



(bus_0) Attributes

Attribute	Value
name	bus_0
model	eth_coax_adv
creation source	Rapid Configuration
creation timestamp	15:55:30 Sep 05 2014
creation data	
right-angled	disabled
label rotation	horizontal
bundle display	include in bundle
ber	0.0
channel count	1
closure model	dbu_closure
coll model	dbu_coll
color	black
condition	enabled
cost	0.0
data rate	10,000,000
delay	0.05
ecc model	dbu_ecc
error model	dbu_error
financial cost	0.00
line style	solid
packet formats	ethernet
propdel model	dbu_propdel
role	
symbol	none
thickness	5
txdel model	dbu_txdel
user id	0

(node_0) Attributes

Type: station

Attribute	Value
name	node_0
model	ethcoax_station
x position	22.8333333333
y position	30
threshold	0.0
icon name	station
creation source	Rapid Configuration
creation timestamp	15:55:30 Sep 05 2014
creation data	
label color	black
⊟ Traffic Generation Parameters	(...)
Start Time (seconds)	constant (5.0)
ON State Time (seconds)	exponential (100)
OFF State Time (seconds)	exponential (0.00001)
⊟ Packet Generation Arguments	(...)
Interarrival Time (seconds)	exponential (2)
Packet Size (bytes)	constant (1024)
Segmentation Size (bytes)	No Segmentation

(pb0) Attributes

Attribute	Value
name	pb0
draw style	linear
group	Traffic Sink
statistic	Traffic Received (packets/sec)
ordinate label	
vector data	enabled
vector start	0.0
vector stop	infinity
scalar data	enabled
scalar type	time average
scalar start	0.0
scalar stop	infinity
capture mode	bucket/default total/sum_time
threshold comparison	disabled
threshold value	0.0
threshold percent	90
tag	none
critical low value	disabled
warning low value	disabled
warning high value	disabled

Rapid Configuration: Bus

Models

Node model: ethcoax_station
Number: 30
Link model: eth_coax
Tap model: eth_tap

Placement

● Horizontal
○ Vertical
☑ Top of bus
☑ Bottom of bus
□ Left of bus
□ Right of bus

Head of bus
X: 20
Y: 50

Size
Bus: 170
Tap: 20

Fig. 13. Configuration of Ethernet Network Nodes.

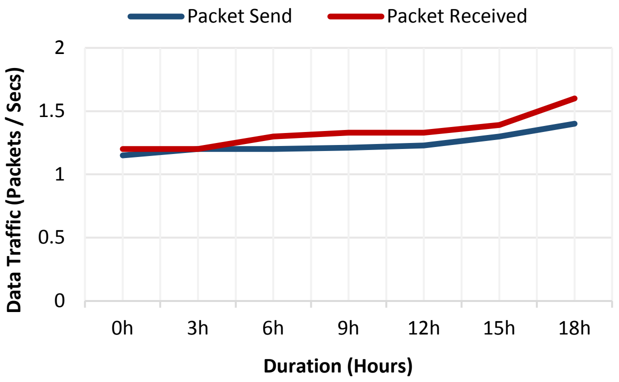


Fig. 14. Data Transferring rate to LBS.

C. Comparative Analysis

In our implementation, we compared the effectiveness of the IDP scheme with DDA concerning different attributes including data transferring rate, Ethernet and Wireless LAN delay, Query success rate, LBS server performance with load, and query processing time, the Route API retransmission attempts and data access rate. These attributes with consequences have been described in the following sections.

1) Measuring data transmission rate: Fig. 15 shows the comparison of the IDP scheme with DDA in terms of data transferring rate. At an initial point, we quantify the data set. When we change the defined dataset, the value of the IDP scheme gradually increases with the increasing time duration, likewise, the value of the DDA scheme also increases with the increasing time duration but its rate is higher than IDP at each defined dataset. it is observed that the data transmission rate of our proposed IDP model is less than DDA. In this case, the frequency at which packets are transferred lower than the DDA scheme. Further, we observed that IDP is better in data transmission as it reduces the collision of data transmission rate significantly.

2) Measuring delay: The delay at Wireless LAN and Ethernet might be the motive of declining LBS server system performance. Fig. 16 shows the comparison between IDP and DDA schemes where delay rate is trivial during query transmission and wireless communication couldn't comprehension to lowering system performance. Fig. 16(a), illustrate that delay in the IDP scheme decreases with less variation as compared to DDA. We also notice, with the increasing time interval both schemes become constant at a certain level. In Fig. 16(b), the change in delay at different time interval in Wireless LAN Delay constitute that IDP delay rate is lesser than the Delay rate in DDA. Hence, the overall delay is decreased.

3) Measuring performance: The fundamental part of the proposed technique was to manage LBS server performance when users posting numerous queries to the system for any POI or any route path to return query results at the server-side. Fig. 17 shows the LBS server performance between the Improved Dummy Position's load processing time and query processing time with the DDA technique. It was also evaluated by [57]. Firstly, the data set is specifying to measure the LBS server performance. The load processing time of LBS server performance in the IDP technique is less than the DDA scheme as shown in Fig. 17(a). On the other hand, the graph of query processing time clearly defines the LBS server takes less processing time in the IDP technique than the DDA scheme as depicted in Fig. 17(b). The performance of IDP is relatively less while the load and query performance time of the DDA scheme is higher and increases gradually.

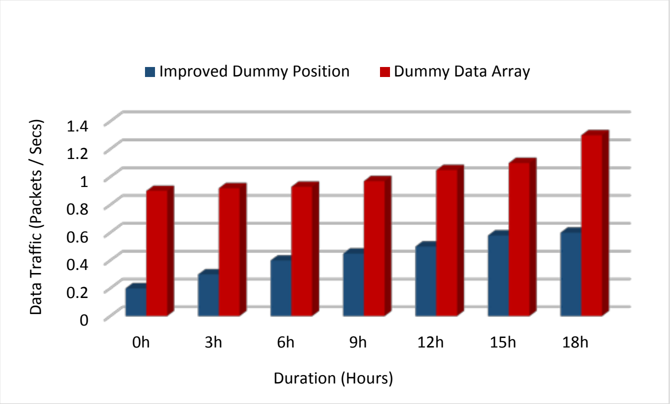
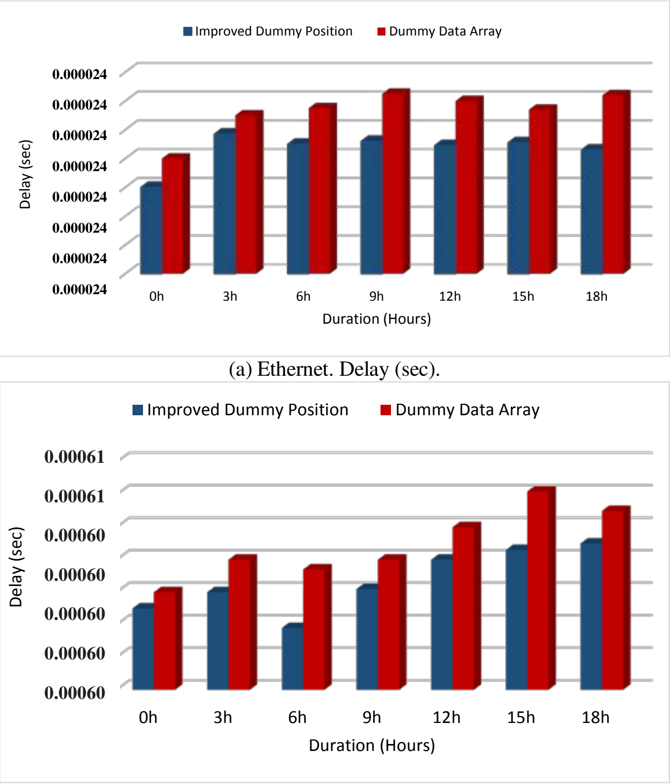


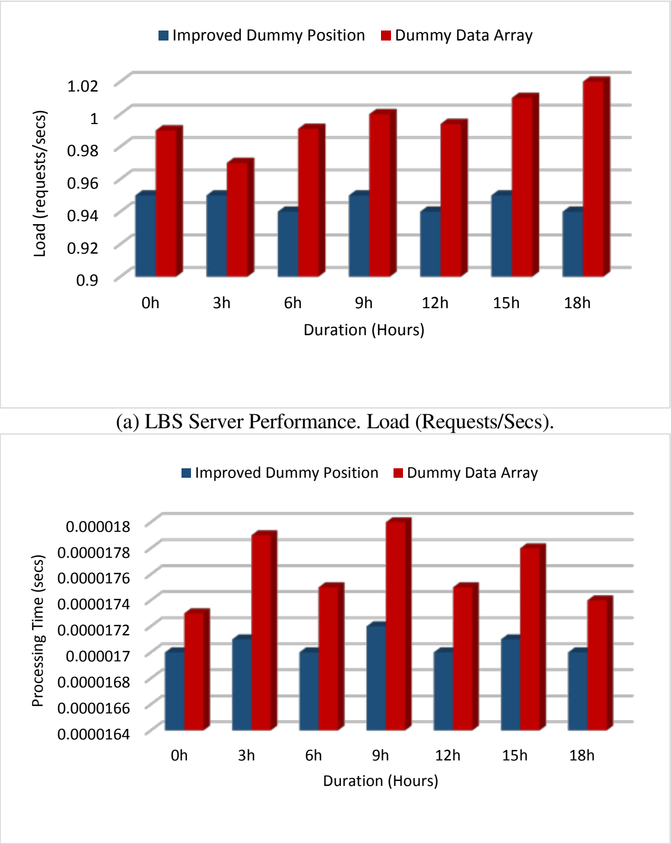
Fig. 15. Comparison on Data Transferring rate to LBS.



(a) Ethernet. Delay (sec).

(b) Wireless LAN. Delay (sec).

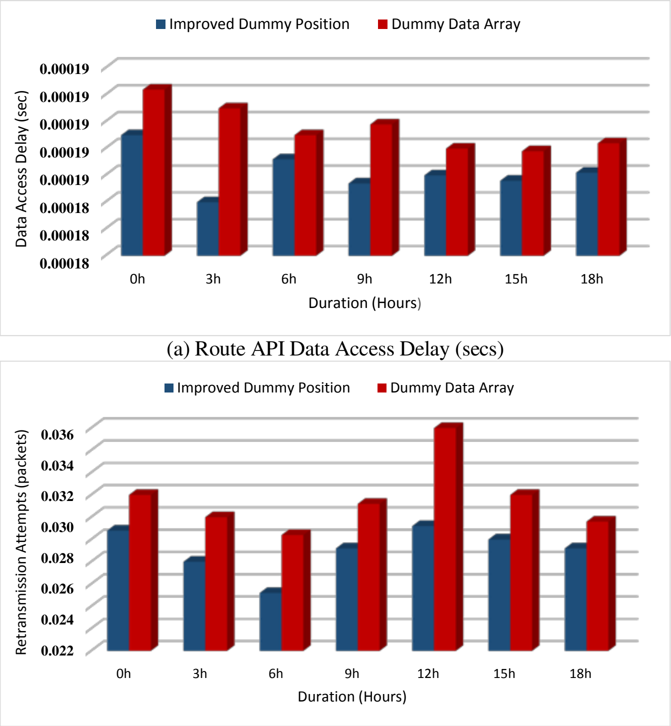
Fig. 16. Delay in Ethernet and Wireless LAN.



(a) LBS Server Performance. Load (Requests/Secs).

(b) LBS Server Performance. Query Processing Time (secs).

Fig. 17. Performance Comparison: LBS Server.



(a) Route API Data Access Delay (secs)

(b) Route API Retransmission Attempts (secs)

Fig. 18. Route API Retransmission Attempts and Data Access Rate.

4) Measuring data access delay and retransmission Attempts: Fig. 18 demonstrates the determination of data access delay through route API [55] and Route API retransmission between Improved Dummy Position and Data Dummy Array schemes. In Fig. 18(a) data access delay of our IDP approach is far better than the existing DDA technique as a tremendous decrease in delay raises when the duration gradually increases. In Fig. 18(b) Route API retransmission of packets is lower than DDA because, an IDP, the LBS server first recognizes the identified path against any packet sent by the TTP LBS user, then provide the accurate local path or point-of-interest (POI).

VI. Discussion

LBS are real-time geographical data from a handheld device that depends on mobile user location to provide information or service. These services allow LBS users to find out required and nearest places such as banks, educational institutions, restaurants, coffee shops, shopping areas, stores, airports, hospitals, cinemas, concerts, and other places or events. Nowadays, the usage of LBS has been increased due to advancements in mobile technology as it requires the geographic location of a mobile user. This leads to serious privacy concerns, as mobile user privacy is at risk. An attacker can take advantage of mobile users' personal information thus the user has to face problems.

In the current study, we highlighted three privacy attributes, user identity, spatial information (position), and temporal information, which need to be protected in order to provide privacy to the LBS user. The privacy of user identity means that a malicious party has access to a location database that contains the actual location of each user but is unable to infer the information about the user from the record because the user is hidden from these untrusted parties. The privacy of the LBS user time of the query is to conceal the temporal information of the user from an attacker so that from time factor actual location of the user could not be disclosed.

An LBS system can be utilized in three ways to provide privacy: Trusted Third Party (TTP), Non-Trusted Third Party (NTTP), and mobile Peer-to-peer networks (P2P). The current study deals with the TTP model where the third party is any server that is assisting LBS to protect the user's private information from disclosure. In TTP LBS System, several privacy provisioning approaches have been recently proposed that are protecting mobile user locations in their way. The main approaches that are ensuring user identity and spatial information are Location Clocking, k-anonymity, Dummy Position, Mix Zone, Policy-based Scheme, Pseudonymisers but the protection of temporal information also required in order to provide full privacy to TTP LBS user. Although all these approaches serve, a great deal for preserving users' privacy still these approaches do not cover all required attributes (Time, Identity, and Position).

To address the privacy challenge under defined metrics, a novel privacy-preserving approach was required. In terms of study objectives, we have conducted a critical analysis of all TTP based approaches and proposed a new model named

Improved Dummy Position "IDP". Leading to objective, we enhanced the dummy position and proposed IDP model that ensures user privacy by changing the user id every time they posted a query to TTP Based LBS System. Based on this model, we design an Improved Dummy Position (IDP) algorithm that takes input user location, anonymity area, and the number of dummies. Anonymity area of user can be grid or circle. The ID has been provided by an additional resource that is a key generator and Sybil Query generates dummies. It returns an array that contains user location and dummies that are indistinguishable. Based on the algorithm, a framework is a design that defines the proper flow of the algorithm.

Further to investigate the privacy rate in the proposed solution, we quantified different privacy attributes through the simulation tool Riverbed Modeller academic edition 17.5. A scenario was created where the size of region A is 200m x 100m. We used Ethernet for simulation and bus topology is constructed consisting of 30 dummy positions/nodes from multiple positions linked with each other and it sends user requests to the LBS system for services. We measured the data transferring rate of the packet sent and received by the LBS server from Ethernet. The consequences showed that the proposed IDP model outperformed the existing state-of-the-art privacy protection techniques by all measured attributes.

Further, we evaluated the IDP model by conducting a comparative analysis with existing models discussed in the literature. In our experiments, we measured delay, performance of LBS server, retransmission, and data access rate. It was observed that IDP brought a tremendous improvement in our results as the success rate of the packet sent and received, improved performance of the LBS server in terms of load and query processing time. The delay in Ethernet and wireless WLAN is less and the retransmission rate of Route API is relatively low. However, IDP results showed that the proposed solution is more efficient than the Data Dummy Array (DDA) algorithm of AES-RS architecture based on measured parameters.

Therefore, the proposed model provides full privacy to TTP LBS user's three attributes (Time, Identity, and Position) and provides a secure environment for getting services from the LBS system. LBS user personal information is released from the service provider and this puts their privacy at risk but relying on the TTP LBS System where anonymised is used to store actual user personal information and protects information from disclosure. Now, the Mobile user fully depends on the TTP Based LBS System without the concern of information exposure.

VII. Conclusion

LBS plays a vital role in emerging mobile computing systems. Leading to TTP based LBS systems, the mobile user is facing some substantial challenges, and privacy is one of these. Fundamentally, a mobile user's privacy is concerned with the user's identity, spatial information, and temporal information. Leading to these privacy attributes, the current study addressed the privacy challenge by proposing a new privacy protection model named "Improved Dummy Position" (IDP) which is the improved version of the dummy position mechanism. In order to make sure the privacy authenticity, we implemented IDP in real France highway road networks using Riverbed modeller academic edition 17.5 simulation tool and measured different privacy factors including Ethernet delay, Query success rate, system performance (load and query processing time), route API retransmission and data access rate. It was observed that IDP outperformed the existing state-of-the-art models and achieved 80% privacy by improving the rate up to 30%. However, this significant improvement provided complete protection in all metrics. From a future perspective, it is crucial to raise the user's focus towards the importance of location privacy and the imperilment when disclosing one's location to third parties. Also, it is required to test the proposed model with real clients with real locations in a real environment with a large system in order to make our contributions stronger.

Acknowledgment

The authors express out their sincere thanks to Prof. Kamal m Jambi for technical and financial support in this research.

References

[1] Puttaswamy, Krishna P. N., Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao. "Preserving Location Privacy in Geo-Social Applications", IEEE Transactions on Mobile Computing, 2012.

[2] M. E. Andrés, N. E. Bordenabe, "Geo-indistinguishability: Differential privacy for location-based system," in Proc. of the 20th ACM Conf. on Computer and Communications Security, pp. 901-914, 2013.

[3] Kang G. Shin, X.J., and Zhigang Chen, X. H. Privacy protection for users of location-based services. IEEE Wireless Communications. 2012.

[4] Mohamad Shady Alrahhal, A. A., Muhammad Usman Ashraf, and S.A. AES-Route Server Model for Location based services in Road Network. (IJACSA) International Journal of Advanced Computer Science and Applications, pp. 361-368, 2017.

[5] M. Duckham and L. Kulik. "A formal model of obfuscation and negotiation for location privacy". In PERVASIVE, 2005.

[6] Tyagi, Amit & Sreenath, N. (2015). A Comparative Study on Privacy Preserving Techniques for Location Based Services. British Journal of Mathematics & Computer Science. 10. 1-25.

[7] Lu Ou, Hui Yin, Zheng Qin, Sheng Xiao, Guangyi Yang, and Yupeng Hu, "An Efficient and Privacy-Preserving Multiuser Cloud-Based LBS Query Scheme," Security and Communication Networks, vol. 2018. 11 pages, 2018.

[8] Alrahhal, Mohamad Shady & Khemakhem, Maher & Jambi, Kamal. (2017). A survey on privacy of location-based services: Classification, inference attacks, and challenges. Journal of Theoretical and Applied Information Technology. 3195.

[9] Available: https://downloads.cloudsecurityalliance.org/. 2018.

[10] Ruchika Gupta and Udai Pratap Rao, "A Hybrid Location Privacy Solution for Mobile LBS," Mobile Information Systems, vol. 2017, Article ID 2189646,11 pages, 2017.

[11] Piao, Chunhui, Xiaoyan Li, Xiao Pan, and Changyou Zhang. "User privacy protection for a mobile commerce alliance", Electronic Commerce Research and Applications, 2016.

[12] Computer Communication Review | acm sigcomm", Sigcomm.org, 2018. [Online]. Available: http://www.sigcomm.org/publications/computer-communication-review.

[13] Ruchika Gupta and Udai Pratap Rao, "A Hybrid Location Privacy Solution for Mobile LBS," Mobile Information Systems, vol. 2017, Article ID 2189646,11 pages, 2017.

[14] Qin Hu Shengling Wang, Chunqiang Hu, Jianhui Huang, Wei Li, Xiuzhen Cheng. "Messages in a Concealed Bottle: Achieving Query Content Privacy with Accurate Location-Based Services", IEEE Transactions on Vehicular Technology, 2018.

[15] Ertaul, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017.

[16] J. Chen, K. He, Q. Yuan, M. Chen, R. Du and Y. Xiang, "Blind Filtering at Third Parties: An Efficient Privacy- Preserving Framework for Location-Based Services," in IEEE Transactions on Mobile Computing.

[17] Aniket Pingley, Wei Yu, Nan Zhang, Xinwen Fu, Wei Zhao “A context-aware scheme for privacy-preserving location-based services”, Computer Networks, 2012.

[18] B. Bamba, L. Liu, P. Pesti, and T. Wang. “Supporting anonymous location queries in mobile environments with privacygrid”. in International Journal of Geo-information, 2008.

[19] C.-Y. Chow and M. F. Mokbel. “Enabling private continuous queries for revealed user locations”. In Security and Communication Networks, 2007.

[20] P. Samarati. “Protecting respondents’ identities in microdata release”. in IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 13, NO. 6, pp. 1010-1027, 2001.

[21] L. Sweeney. “K-anonymity: A model for protecting privacy”. IJUFKS, pp, 557–570, 2002.

[22] Hidetoshi Kido, Y. Y., & Satoh, T. “Protection of Location Privacy using Dummies for Location-based Services.”. Proceedings of the 21st International Conference on Data Engineering (ICDE ’05) , 2005.

[23] C.-Y. Chow, M. F. Mokbel, and X. Liu. “A peer-to-peer spatial cloaking algorithm for anonymous location-based services”. In ACM GIS, 2006.

[24] Mohammad Yamin, Adnan Ahmed Abi Sen. "Improving Privacy and Security of User Data in Location Based Services", International Journal of Ambient Computing and Intelligence, 2018.

[25] Wernke, Marius, Pavel Skvortsov, Frank Dürr, and Kurt Rothermel. “A classification of location privacy attacks and approaches”, Personal and Ubiquitous Computing, 2014.

[26] Marius Wernke, P. S., & Frank Du¨rr, K. R. “A Classification of Location Privacy Attacks and Approaches”, pp, 1-24.

[27] Chi-Yin Chow, M. F. (n.d.). “Privacy in Location-based Services: A System Architecture Perspective”, pp, 23-27.

[28] OPUS: Zur Startseite”, Elib.uni-stuttgart.de, 2018. Available: https://elib.umi-stuttgart.de/.

[29] “Location Based Services”, Available: pooh.poly.asu.edu/Mobile/ ClassNotes/.../LocationBasedSvcs/LocationBasedServices.

[30] Robert Kolvoord, K. K., & Rittenhouse, P. “Applications of Location-Based Services and Mobile”. International Journal ofGeo-information, pp: 1-9. 2017.

[31] Michael, K. “Location-Based Services: a vehicle for IT&T convergence”, pp: 467-477. 2004.

[32] Ertaul, L. “Privacy in Location Based Services (LBS) via Composite Privacy in Location Based Services (LBS) via Composite Privacy in Location Based Services” . IJCSNS International Journal of Computer Science and Network Security, pp:117-123. 2017.

[33] Costas Pontikakos, T. G., & Tsiligiridis, T. “Location-based services: architecture overview”, 2015.

[34] Neeta B. Bhongade, G. P, “A Review of Privacy Preserving LBS: Study of Well-Suited Approaches,” in International Journal of Engineering Trends and Technology (IJETT), pp. 62-65. 2015.

[35] Gruteser, M., Grunwald, D, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys ’03), New York, NY, USA, ACM, pp. 31–42. 2003.

[36] Mokbel, M.F., Chow, C.Y., Aref, W.G, The new casper: query processing for location services without compromising privacy,” in Proceedings of the 32nd international conference on Very large data bases (VLDB ’06), VLDB Endowment, pp. 763–774. 2006.

[37] Gedik, B., Liu, L, “Location privacy in mobile systems: A personalized anonymization model,” in International Conference on Distributed Computing Systems (ICDCS), pp. 620–629. 2005.

[38] Gedik, B., Liu, L, “Protecting location privacy with personalized k-anonymity: Architecture and algorithms,” in IEEE Transactions on Mobile Computing 7, pp. 1–18. 2008.

[39] Zhang, C., Huang, Y, “Cloaking locations for anonymous location based services: a hybrid approach,” in Geoinformatica 13, pp. 159–182. 2009.

[40] Bamba, B., Liu, L., Pesti, P., Wang, T, “Supporting anonymous location queries in mobile environments with privacygrid,” in Proceeding of the 17th international conference on World Wide Web (WWW ’08), New York, NY, USA, ACM, pp. 237–246. 2008.

[41] Li, N., Li, T., Venkatasubramanian, S, “t-closeness: Privacy beyond k-anonymity and l-diversity,” in Proceedings of the IEEE 23rd International Conference on Data Engineering (ICDE), pp. 106–115. 2007.

[42] Solanas, A., Seb´e, F., Domingo-Ferrer, J, “Micro-aggregation-based heuristics for p sensitive k-anonymity: one step beyond,” in Proceedings of the 2008 international workshop on Privacy and anonymity in information society (PAIS ’08), New York, NY, USA, ACM, pp. 61–69. 2008.

[43] Mascetti, S., Bettini, C., Wang, X.S., Freni, D., Jajodia, S: Providenthider, “An algorithm to preserve historical k-anonymity in lbs,” in IEEE International Conference on Mobile Data Management (MDM 2009). Volume 0, Los Alamitos, CA, USA, IEEE Computer Society, pp. 172–181. 2009.

[44] Kido, H., Yanagisawa, Y., Satoh, T, “An anonymous communication technique using dummies for location-based services,” in Proceedings of the International Conference on Pervasive Services (ICPS), pp. 88–97. 2005.

[45] Shankar, P, Ganapathy, V., Iftode, L, “Privately querying location-based services with sybilquery,” in International Conference on Ubiquitous Computing (UbiComp), 2009, pp. 31–40.

[46] Beresford, A.R, Stajano, F, “Mix zones: User privacy in location-aware services,” in PerCom Workshops, pp. 127–131. 2004.

[47] Palanisamy, B., Liu, L, “Mobimix: Protecting location privacy with mix-zones over road networks” in Proceedings of the 2011 IEEE 27th International Conference on Data Engineering. ICDE ’11, Washington, DC, USA, IEEE Computer Society, pp. 494–505. 2011.

[48] Agusti Solanas, J. D.-F.-B.“Location Privacy in Location-Based Services: Beyond TTP-based Schemes”.

[49] H. L. C. S. Jensen and M. L. Yiu, "PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services," ACM, 2008.

[50] Z. Z. Ben Niu and H. L. Xiaoqing Li, "Privacy-Area Aware Dummy Generation Algorithms for Location-Based Services," IEEE ICC 2014 - Communication and Information System Security Symposium, pp. 957-962. 2014.

[51] Hidetoshi Kido, Y. Y., & Satoh, T, “Protection of Location Privacy using Dummies for Location-based Services,” in International Conference on Data Engineering, 2005.

[52] A. Civilis, C.S. Jensen, and S. Pakalnis. “Techniques for efficient roadnetwork-based tracking of moving objects.”Knowledge and Data Engineering, IEEE Transactions on 17.5, pp: 698-712. 2015.

[53] Riverbed Modeler Academic Edition 17.5 available and Download: https://cms-api.riverbed.com/portal/community_home

[54] [54] Little, D.C. John, and C.G. Stephen. “Little's law.” Building Intuition. Springer US, 2008. 81-100.

[55] L. Yu and M. Y. Lung. “Route-Saver: Leveraging Route APIs for Accurate and Efficient Query Processing at Location-Based Services.” Knowledge and Data Engineering, IEEE Transactions pp: 235-249. 2015.

[56] Muhammad Usman Ashraf, Rida. Qayyum, & Ejaz, H, "State-of-the-Art, Challenges: Privacy Provisioning in TTP Location based Services Systems", International Journal of Advanced Research in Computer Science, Volume 10, No. 2, pp. 68-75, 2019.

[57] Alrahhal, Mohamad Shady, Maher Khemekhem, and Kamal Jambi. "Achieving load balancing between privacy protection level and power consumption in location based services." (2018).

[58] Alrahhal, Mohamad Shady, Maher Khemakhem, and Kamal Jambi. "Agent-Based System for Efficient kNN Query Processing with Comprehensive Privacy Protection." International Journal of Advanced Computer Science and Applications 9.1 (2018): 52-66.

[59] Alrahhal, Mohamad Shady, Maher Khemakhem, and Kamal Jambi. "A Survey on Privacy of Location-Based Services: Classification, Inference

Attacks, and Challenges." Journal of Theoretical and Applied Information Technology 95.24 (2017).

[60] Qaiser, S., Bukhari, S. A., Zainab, W., & Ashraf, M. U. (2019). Privacy provision for TIP attributes in NTTP Based LBS Systems. International Journal of Advanced Research in Computer Science, 10(2), 84.

[61] Alsubhi, Khalid, M. Usman Ashraf, and Iqra Ilyas. "HBLP: A Privacy Protection Framework for TIP Attributes in NTTP-Based LBS Systems." IEEE Access 8 (2020): 67718-67734.

[62] Ashraf, Muhammad Usman, et al. "H2E: A Privacy Provisioning Framework for Collaborative Filtering Recommender System." International Journal of Modern Education & Computer Science 11.9 (2019).

[63] Ashraf, Muhammad Usman, Iqra Ilyas, and Farzana Younas. "A Roadmap: Towards Security Challenges, Prevention Mechanisms for Fog Computing." 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE, 2019.

[64] Ashraf, Muhammad Usman, et al. "Provisioning quality of service for multimedia applications in cloud computing." Int. J. Inf. Technol. Comput. Sci.(IJITCS) 10.5 (2018): 40-47.